2010-03

Network exploration and vulnerability assessment using a combined "blackbox" and "whitebox" analysis approach

Choong, Patrick Wee Meng

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/5388

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NETWORK EXPLORATION AND VULNERABILITY ASSESSMENT USING A COMBINED "BLACKBOX" AND "WHITEBOX" ANALYSIS APPROACH

by

Patrick Choong Wee Meng

March 2010

Thesis Advisor:	Geoffrey Xie
Thesis Co-Advisor:	John Gibson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Network Exploration and Vulnerability Assessment Using A Combined "Blackbox" and "Whitebox" Analysis Approach	**5. FUNDING NUMBERS** N/A
6. AUTHOR(S) Patrick Choong Wee Meng	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER** N/A

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.
IRB Protocol number _____N/A___________.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The increased reliance on advanced networking technologies to integrate cutting-edge capabilities has posed tremendous challenges in assuring user legitimacy and preserving the integrity of our network landscape. Without proper network accountability and holistic vulnerability assessment, insider threats can exploit the security vulnerabilities that result from creating an integrated system-of-systems. To detect security illegitimacies, such as unauthorized connections, network security administrators need to have a comprehensive network map to identify potential entry points.

This thesis proposes a systematic way to combine "black-box" and "white-box" analysis for network exploration and vulnerability assessment. In the analytical model design, a modular approach is adopted to select tools and techniques from both analysis approaches. These tools and techniques are used to construct a network map based on a pre-defined set of criteria that define the type of essential network information to be annotated on the map. The "black-box" and "white-box" analysis approaches were found to be complementary. For example, "black-box" analysis was able to map active hosts and networking devices, but "white-box" analysis was able to detect those that are inactive or do not respond to pings. Moreover, "black-box" analysis provides a focal point for "white-box" analysis approach to derive in-depth information regarding unauthorized connections.

14. SUBJECT TERMS Network Exploration, Black-box Analysis, White-box Analysis, Vulnerability Assessment	**15. NUMBER OF PAGES** 75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

NETWORK EXPLORATION AND VULNERABILITY ASSESSMENT USING A COMBINED "BLACKBOX" AND "WHITEBOX" ANALYSIS APPROACH

Patrick Choong Wee Meng
Major, Republic of Singapore Air Force
Bachelor of Engineering (Hons) (Mechanical Engineering),
University of New South Wales, Australia, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Author: Patrick Choong Wee Meng

Approved by: Geoffrey Xie
Thesis Advisor

John Gibson
Co-Advisor

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The increased reliance on advanced networking technologies to integrate cutting-edge capabilities has posed tremendous challenges in assuring user legitimacy and preserving the integrity of our network landscape. Without proper network accountability and holistic vulnerability assessment, insider threats can exploit the security vulnerabilities that result from creating an integrated system-of-systems. To detect security illegitimacies, such as unauthorized connections, network security administrators need to have a comprehensive network map to identify potential entry points.

This thesis proposes a systematic way to combine “black-box” and “white-box” analysis for network exploration and vulnerability assessment. In the analytical model design, a modular approach is adopted to select tools and techniques from both analysis approaches. These tools and techniques are used to construct a network map based on a pre-defined set of criteria that define the type of essential network information to be annotated on the map. The “black-box” and “white-box” analysis approaches were found to be complementary. For example, “black-box” analysis was able to map active hosts and networking devices, but “white-box” analysis was able to detect those that are inactive or do not respond to pings. Moreover, “black-box” analysis provides a focal point for “white-box” analysis approach to derive in-depth information regarding unauthorized connections.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is dedicated to my wife, Jessie, who has shown tremendous support and kind understanding on the amount of time I had to spend in completing my research work. Her relentless encouragement and emotional support has always been the key motivator in pushing me to give my fullest and make the best out of this thesis work. She has helped me untangle the difficult times that I had during the time of my study at Naval Postgraduate School.

I want to express my greatest gratitude to Professor Geoffrey Xie for giving me the opportunity to work on a topic of my choice, trusting me to work independently in my research work, and completing this piece of thesis work in time despite the heavy workload each quarter. His valuable insights and guidance have never failed to steer me back on course in my research work.

My greatest appreciation goes out to my co-advisor, Mr. John Gibson who have shown me the ropes in mastering a new skill in my course of study – setting up a network from scratch as my thesis test-bed. I thank him for his kind patience in the painful process of debugging the host and router configurations.

I owe this heart-felt opportunity of pursuing a Master’s in Computer Science to Brigadier General Lee Shiang Long (Singapore Army), Colonel Yong Yoke Chuang (Republic of Singapore Air Force), and Lieutenant-Colonel Hong Kian Wah (Singapore Navy). They have shown the greatest support for my persistent eagerness to pursue an academic area, which I have no relevant background in. My ability to shorten my coursework and complete this thesis work in time is not possible without their constant encouragement and motivation.

Finally, I want to thank my classmates—Captain Joshua Dixon (U.S. Marine Corp), Lieutenant Dennis Holden (U.S. Navy), and Lieutenant Junior Grade Mark Bergem (U.S. Navy) for their constant emotional support in Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The impact of cyberspace on the commercial and financial sectors influenced military operations to increase their capitalization of advanced networking technologies and, thereby, reap key benefits of information technology. In June 2009, U.S. Defense Secretary Gates issued a memorandum to establish the U.S. Cyber Command for military cyberspace operations and asserted that cyberspace will become a dominant enabler in military operations.

> Cyberspace and its associated technologies offer unprecedented opportunities to the United States and are vital to our Nation's security and, by extension, to all aspects of military operations. Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. [1]

The developments of war-fighting concepts have evolved from platform-centric development to network-centric force development. They focus on creating integrated sensor-shooter capabilities and fighting as an integrated, networked force. Key enabling networking technologies, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Web services, and network devices, like routers, steered the stove-piped posture of operational systems to a tightly integrated global computing ecosystem.

Integrating stove-piped and proprietary legacy systems was a challenging up-hill task, let alone integrating it with new systems. Introduction of new architectural framework to define and deliver net-centric capability from legacy military systems [2] and software technologies such as the Net-Centric Adapter for Legacy Systems (NCALS) [3] was necessary. It was relatively easy to assess the security of systems individually, and account for the supporting network devices to identify potential entry points into the network. However, it becomes more challenging to assess the overall security posture when these systems are integrated. Accountability of the enabling network devices became time-consuming as the network landscape grew exponentially when large networks are integrated. Furthermore, the security challenges increase dramatically when individual networked systems are integrated with other networked systems to form a larger system-of-systems. Introduction of new interdependent vulnerabilities is possible and requires a holistic vulnerability assessment to mitigate them.

Authenticating the legitimacy of network devices and preserving the integrity of the network landscape is paramount because it is the key enabler for our critical operational capabilities. This involves accounting for every key networking device that enable the close integration of systems to detect illegitimate host or router connections made possible by insider threats [4]. Insider threats may connect unauthorized computer systems or routers to publicly accessible switch ports and establish authorized connections, which they may launch attacks or accidentally leak sensitive information out from the closed network. Traditionally, vulnerability assessments or penetration testing can reveal potential entry points on networks. As the network landscape grows continually with more integration of large system-of-systems, there is a need for a holistic vulnerability assessment to identify vulnerabilities at the system level. It should be comprised of a comprehensive suite of vulnerability assessment techniques and tools that are able to conduct comprehensive vulnerability assessment when these system-of-systems are integrated. This will minimize the security risks of insider threats exploiting these entry points as a venue for their attacks on the network. Proper network accountability will eventually prevent the escalation of such attacks because clusters of compromised computer networks can be more responsively isolated and recovered.

A. OBJECTIVE

Current discovery techniques, including human knowledge and physical inspection [5], are encouraged for network exploration, but it has proved to be time-consuming and faced tremendous challenges in updating the database.

There is a need for an efficient way to aid the network security administrators in addressing the issue of network accountability as part of vulnerability assessment.

An integrated approach is adapted in this thesis to propose a way to address the issue of proper network accountability and comprehensive assessment. It leverages on the strengths of the “black-box” analysis approach to address the challenges in accounting networking devices in an unknown, composite system-of-systems environment, and the comprehensiveness of a “White-box” analysis approach to advance our knowledge of our existing component networks. By mapping the entire system-of-systems into a network map, the map will provide a complete picture for the conduct of a holistic vulnerability assessment at the system level.

The thesis intends to develop an analytical model to produce a more comprehensive network map with which holistic vulnerability assessment is made to detect unauthorized host and router connections that are connected via publicly accessible switch ports. It will pave the way for the future development of an application program to perform comprehensive network exploration and vulnerability assessment for large, unknown or poorly documented systems-of-systems. This research will assist the network security administrators to better understand the risks of insider threats, so that they can develop more responsive security policies and measures to recover compromised systems.

B. BENEFITS OF AN INTEGRATED APPROACH

The “Black-box” approaches that were adapted involve understanding the behavior, capabilities and limitations of current network mapping techniques, such as Network Mapper (Nmap) [6] and Nessus [7]. Because such techniques do not require prior knowledge of a system-of-systems and its supporting networks, they were useful for mapping the current network state at which network devices are connected.

“Black-box” analysis techniques can aid determining what hosts are available on the network, the services these hosts are offering, the types of operating systems they are running, and other characteristics that are useful for identifying a host or a network device. However, this approach has its limitations because there is no way by itself to validate the completeness of its assessment or determining what it has not discovered. By contrast, a “white-box” analysis approach starts with some knowledge of the characteristics of the system-of-systems. However, this knowledge can become outdated as large system-of-systems are integrated at a fast-paced system integration cycle that strives to meet functionalities of critical mission requirements.

The key benefits in combining the “black-box” analysis approach with the “white-box” analysis approach were two fold (1) the two approaches complement each other’s strengths and limitations to conduct network exploration and vulnerability assessment, and (2) it proposes a systematic way to combine “black-box” and “white-box” analysis approaches.

C. RESEARCH QUESTIONS

The primary research question that this thesis endeavors to answer is “What will the integrated approach of combining “black-box” and “white-box” analysis entail to discover unauthorized host and router connections?” Other subordinate issues include:

a. What are the limitations in current network exploration and vulnerability assessment techniques for an unknown system-of-systems?

b. How many more network vulnerabilities can we discover combining “black-box” and “white-box” analysis approaches?

c. What are the parameters used to ascertain that there are unauthorized host and router connections in the system-of-systems?

d. What are the benefits of adopting this integrated approach for mapping an unknown system-of-systems?

D. THESIS ORGANIZATION

Chapter II provides an overview of the current network exploration and vulnerability assessments techniques used in the “black-box” and “white-box” analysis approaches. It discusses the limitations of employing these approaches to conduct network exploration and vulnerability assessment.

Chapter III presents the integrated approach of combining “black-box” and “white-box” analysis approaches, and compares its impact on network exploration and vulnerability assessment with current techniques.

Chapter IV covers the analytical model for discovering unauthorized host and router connections, using the proposed integrated approach.

Chapter V summarizes the thesis efforts and provides recommendations for follow-up research, specifically in the development of an application program that automatically conducts network exploration and vulnerability assessment using the proposed integrated approach.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. PROLOGUE

This chapter provides a quick overview of the key developments in network exploration and vulnerability assessment for a large integrated system-of-systems. The focus of this literature review is on current tools and techniques in three sections, namely: network exploration, detection of unauthorized connections by insider threats, and vulnerability assessment, as depicted in Figure 1. There are tools and techniques that are currently used to map known and unknown (also commonly known as vulnerabilities subjected to Zero-day attacks) vulnerabilities, in relation to the networked environment.

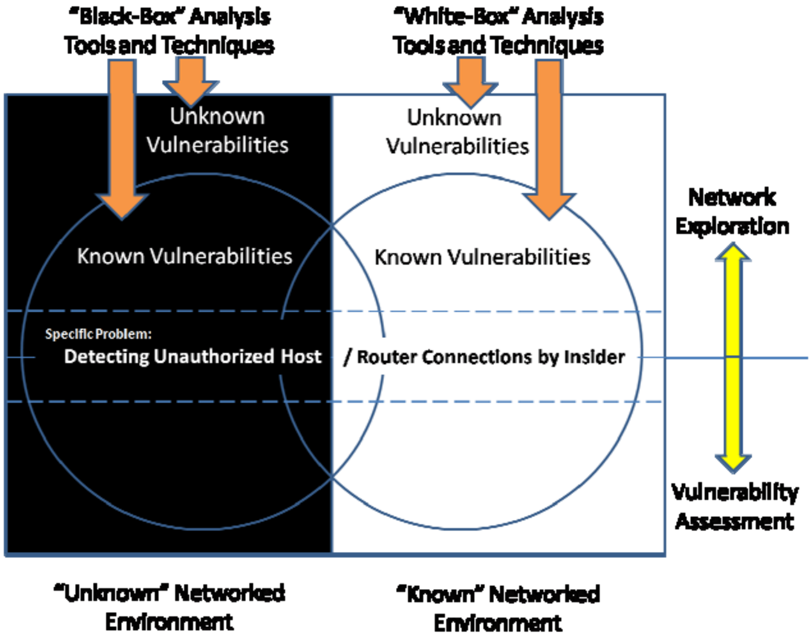

"Black-Box" Analysis Tools and Techniques
"White-Box" Analysis Tools and Techniques
Unknown Vulnerabilities
Unknown Vulnerabilities
Known Vulnerabilities
Known Vulnerabilities
Network Exploration
Specific Problem:
Detecting Unauthorized Host
/ Router Connections by Insider
Vulnerability Assessment
"Unknown" Networked Environment
"Known" Networked Environment

Figure 1. Focus Areas of Literature Review

In mapping unknown environments and validating the integrity of known ones, this review discusses the scope and capabilities of these known techniques. With specific scenarios crafted to model the problem of detecting unauthorized connections made by insider threats, current network monitoring and intrusion detection techniques are also reviewed to understand what they can or cannot detect. System vulnerabilities resulting from integrating large networked systems is an emerging security issue and there are related research efforts that will aid in modeling the integrated approach in this thesis.

B. “BLACK-BOX” ANALYSIS VERSUS “WHITE-BOX” ANALYSIS

“Black-box” analysis refers to analyzing an unknown network topology by probing it with various input data packets to elicit responses from hosts that are operating on the network (also known as “live” hosts). From the hacker’s perspective, this is similar to a commonly known process called Network Reconnaissance or Fingerprinting, whereby tools such as Nmap, and Xprobe2 [8] are used to generate a list of vulnerable targets for the hacker to plan his attack. The target list will consist of a network map that details vulnerable hosts and networking devices, as well as their network information such as IP addresses and operating system versions. “Black-box” analysis is easier to perform because it does not require as much expertise as compared to “white-box” analysis. In terms of obtaining knowledge from the network, it is not as effective as “white-box” analysis because it heavily relies on the responses it received from running hosts and networking devices.

On the other hand, “white-box” analysis refers to analyzing and validating the status and inventory of a known network environment. It is usually associated with Network Management and Monitoring tools such as LANsurveyor [9] that help the network administrators maintain the integrity of the network. Other “white-box” analysis techniques include detailed examination of configuration files and states of the edge networking devices such as routers and switches. In terms of obtaining knowledge for completeness, this approach is very effective because it deals with known network environments and network information is readily accessible. The main drawback in the “white-box” analysis approach is the relatively high false positive rates as compared to “black-box” analysis. By virtue that the scope of the network is large and it takes time to ensure network integrity (such as disseminating the latest security patches) and ensure inventory accountability, network information can get outdated frequently as the network environment is periodically evolving.

C. CURRENT NETWORK EXPLORATION TECHNIQUES

Advanced militaries continue to leverage networking technologies and integrate networked systems-of-systems at a fast-paced development cycle, and this poses great challenges for the network administrators and security managers to keep pace and grasp the overall network architecture and system vulnerabilities in a constantly changing security landscape. The “fog of war” has increased in the cyberspace domain and extended beyond the scope of network mapping. Traditionally, network mapping is a technique associated with a hacker attempting to determine the hosts or services available in a target network. This will allow him to determine the host that is the weakest link, offering a gateway to launch his attack into the network. From the network monitoring perspective, a network administrator will need to have comprehensive network topology information at hand to determine the availability and security status of his network, to respond quickly to incidents that vary from system failures to cyber attacks. This information will also aid in the Information Technology (IT) audit process.

Network Exploration is a term adapted for this thesis to represent the process of gaining knowledge about the defended network in order to assure network integrity in the presence of hostile actions. It works on the assumption that there is zero knowledge about the target system-of-systems and subsequently employing a systematic approach to explore and map out all computers and networking devices. Unlike network mapping from the perspective of a hacker, network exploration does not primarily focus on vulnerable systems in its network but attempts to map the entire cyberspace that enables critical networked operation of the system-of-systems. The network map generated by this process will comprise hosts, servers, and networking devices, in both wired and wireless domains, that make up the enabling cyberspace. The techniques used to construct network diagrams of an unknown network environment are usually in the realms of network reconnaissance and network management and monitoring.

1. Network Reconnaissance

Network reconnaissance techniques are essential for an attacker to determine the vulnerabilities of the network stealthily. They are categorized as either active or passive reconnaissance. Passive network reconnaissance involves the collection of network information through social engineering and publicly available information. However, these techniques are not relevant because the nature of our military operational networks is usually confidential and not publicly available. Comparatively, active reconnaissance involves techniques that generate network traffic to elicit responses from the target network. These responses are relatively real-time and more informative in generating a detailed network map, which is useful for identifying unauthorized host and router connections. The techniques and tools of direct relevance are:

a. Nmap (Network Mapper)

The most common network exploration tool for mapping an unknown environment is Nmap, as it is designed to scan large networks rapidly. Nmap can explore an unknown network by running combinations of multi-port scans on several network protocols to determine if there are hosts available on a specified Internet Protocol (IP) address. If the hosts do not respond to the data packets (or “pings”) sent out by Nmap, it will interpret that no host or network device uses the scanned IP addresses. Nmap supports host discovery based on the responses it receives. It analyzes them, builds a signature for that host, and compares the host’s signature with its database to determine the host’s operating system, the services it offers, and other characteristics that can attribute to differentiating a host from another network device.

b. Xprobe2++

The design of Xprobe2++ focused on employing remote network scanning on both the network and application layers of an unknown target network to build up a host signature based on collected responses. Xprobe2++ is able to identify the type and version of the operating system that the detected host is using. It is an improvement from its predecessor, Xprobe2, increasing its host detection capability via a better signature engine and fuzzy signature matching process. Significant enhancements have made the probing capability of Xprobe2++ stealthier by minimizing the network traffic overhead of its data packets. Its host discovery modules are designed to perform host probing, firewall detection, and provide additional information to estimate the actual response time and identify packets dropped by the detected host. Comparatively, Xprobe2++ proved that it generates less traffic loads than Nmap when no TCP port scanning is performed [10].

2. Network Management and Monitoring

Techniques and tools that support network management and monitoring are employed on known network environments and primarily focus on maintaining network integrity, planning resource and capacity usage, and monitoring network performance. Some advanced network management tools will provide network-mapping capability and may be used by network administrators to track IP addresses, and configure network devices and systems. In terms of monitoring performance, network management tools employ techniques to determine if optimization is in place for the network's performance. These network-mapping tools include:

a. LANsurveyor

LANsurveyor is an automatic network-mapping tool that discovers active hosts and network devices from an unknown environment using multi-discovery techniques. It sends out Simple Network Management Protocol

(SNMP) pings and scans to Active Directory Domain Controllers that contain information about network services, such as the Lightweight Directory Access Protocol (LDAP) directory services and DNS-based naming information. LANsurveyor is able to monitor the network and dynamically update the network map with new devices and unknown systems that are active on the network. Upon detection of unknown or rogue connections, LANsurveyor can automatically disable the network access for that device. The spanning tree support for LANsurveyor enables it to provide accurate mapping of switch-to-switch connectivity.

b. IPSonar

IPSonar is another advanced network-mapping tool that aims at providing global visibility of known networks and evaluates security risks from a network administrator’s perspective. Its network-mapping capability involves mapping every host and network device on a network, including those that are currently not under its management. This is to provide visibility of the connectivity between hosts/network devices and the underlying supporting networks, so that the administrators can analyze the potential security risks and attack patterns. IPSonar extends its capability to encompass identification of network bottlenecks due to poor configurations and vulnerabilities exploitable by unknown devices.

D. RELATED WORK IN DETECTING UNAUTHORIZED CONNECTIONS

Research on insider threats spans across wide areas of network security, especially in the area of detecting malicious activities by insiders. The common solution to combat malicious activities generated by insider threats is the employment of Network Intrusion Detection Systems (NIDS) that examine traffic data against its signature database or known heuristics to discern malicious from legitimate traffic. It is noticeable that such detection techniques are reactive in nature and there exists great challenges in maintaining high accuracies in detecting true malicious traffic in the network [9]. There is a need for a more responsive approach in detecting unauthorized connections.

1. Overview

In this section, the focus of the literature review is on three specific scenarios to illustrate how current detection capabilities address the detection of unauthorized host and router connections. The first scenario entails the attacker attempting to connect an unauthorized host into one of the readily available switch ports (unsecured wall-jack access) and launch his attack on un-patched and vulnerable networked systems. In the second, the attacker can extend the network coverage to create his/her unauthorized wired and wireless networks with which attacks can be coordinated and launched. Finally, the attacker can simply connect an unauthorized wireless access point to provide subsequent access into a physically hardened network.

2. Unauthorized Host and Router Connections

In this first scenario, as illustrated in Figure 2, the attacker simply uses readily available switches, or exposed wall-jack connections to switches, located in the public access areas to establish an unauthorized host connection.

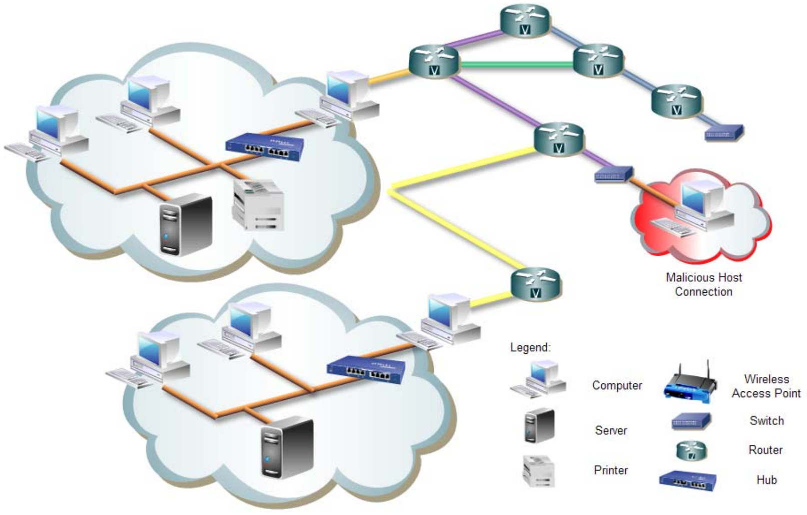


Figure 2. Unauthorized Host Connection

From this unauthorized connection, the attacker will scan for network vulnerabilities, and launch a variety of network attacks that range from introducing viruses to performing denial of service attacks on vulnerable systems. Detection of a new host or router in the network can be achieved by using network-monitoring tools that generate network maps, such as LANsurveyor and IPSonar. These tools automatically update the network maps if there are changes to the network topology, including the unauthorized host and router connection. However, these tools cannot determine the malicious activities in isolation without any vulnerability assessment capabilities built-in or provided by another tool.

Figure 3 depicts a scenario in which the attacker connects a router and sets up his/her own wired and wireless networks. These hosts are likely to introduce vulnerabilities to the original network, as they do not meet the security requirements. In a worst-case scenario, the attacker may use it to leak sensitive or classified information out to the wireless networks and/or as a launch pad to coordinate distributed denial-of-service attacks.

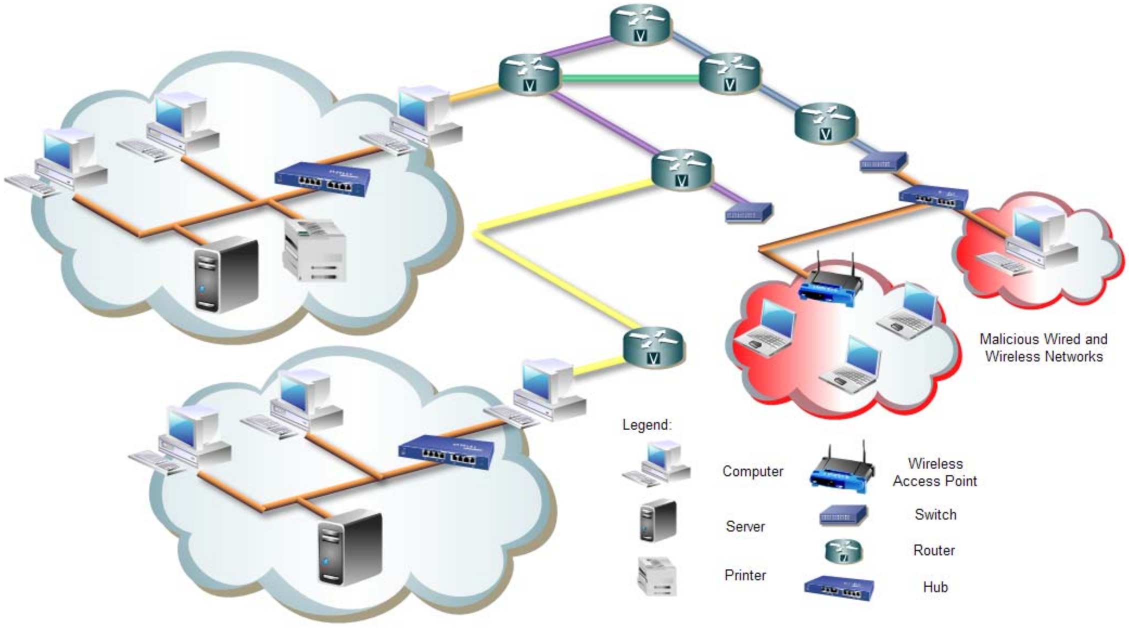


Figure 3. Unauthorized Router Connection

3. Unauthorized Wireless Access Point Connections

As depicted in Figure 4, this is a scenario whereby the attacker connects a wireless access point as a legitimate entry point, but it also serve as a malicious platform waiting to be exploited for subsequent attacks ranging from network inject to denial-of-service attacks. Wireless networks provide high mobility and extensibility of Internet access through wireless access points that are radio transmitters and receivers. As the transmission of data uses radio frequencies that are omni-directional, many research studies have shown that wireless access points and wireless networks have inherent vulnerabilities that are exploitable by attackers. Thus, the ability to detect unauthorized wireless access points in a secured environment is essential to maintaining network security.

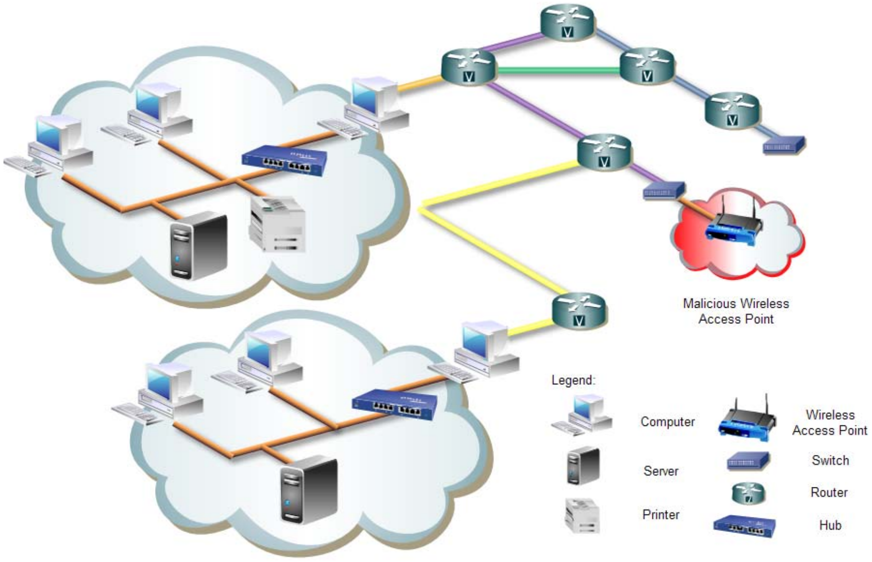


Figure 4. Unauthorized Wireless Access Point

The detection of unauthorized wireless access points (or more commonly known as Rogue Wireless Access Points (RWAPs)) can employ two potential architectural options, namely “Over the Air” architecture and “Over the Wire” architecture, as described in [10]. The “Over-the-Air” architecture and scanning techniques evolved from scanning the network physically to installing permanent listening devices or sensors and instituting portable sensor zones that are adjustable based upon recognition of client messages to reduce sensor density, and thereby cost and maintenance, while providing the desired detection capability. The “Over-the Wire” architecture and detection techniques require gathering of network information from cooperation with connected network devices, to detect a malicious RWAP. This falls back to our discussion on current network exploration techniques that can be used for detecting such devices.

Other research in this area involves employing different techniques, such as the Rouge Identifying Packet Payload Slicer (RIPPS) [11], to improve this detection capability. Essentially, this new technique detects RWAPs without using wireless sensors or deploying any host-based listening devices. It leverages on the combined effectiveness of active network traffic conditioning techniques with passive packet timing analysis to enhance the accuracy and speed of its detection measurements.

E. CURRENT VULNERABILITY ASSESSMENT TECHNIQUES

1. Vulnerability Assessment Tools and Techniques

There are a vast number of vulnerability assessment tools that focus on determining if hosts are patched with the latest security updates, and/or misconfigured. However, the review focuses on those that are relevant in contributing to assessing large system-of-systems.

a. Nessus

Nessus is a well-known vulnerability assessment tool designed to automate the testing and discovery of known security vulnerabilities of a network. It has the ability to detect remote flaws, local flaws and missing patches of the hosts on the network. The Nessus security scanner uses NASL (Nessus Attack Scripting Language) to write its own security tests as a plug-in, thereby the administrators need not download untrusted binaries from the Internet. In addition, this tool recognizes services that are run on a non-standard port assigned by Internet Assigned Numbers Authority (IANA). The vulnerability assessment involves three phases, namely: Scanning, Enumeration and Vulnerability Detection. These phases allow Nessus to scan for hosts that are operating on the network, determine the services that are run on the host and networking devices, and checks for vulnerabilities based on known vulnerabilities, such as buffer-overflows and improper configuration etc.

2. System-level Vulnerability Assessment

The problem of detecting unauthorized host and router connections becomes more complex when collections of independent systems are integrated to form a large system-of-systems, and the underlying networks grow non-linearly due to interconnections between the component systems. In addition, such integration processes may generate vulnerabilities that are unknown to developers and security engineers from each component systems. Such vulnerabilities may be a result of network security conflicts or inheritance of unknown system vulnerabilities, as illustrated in Figure 5.

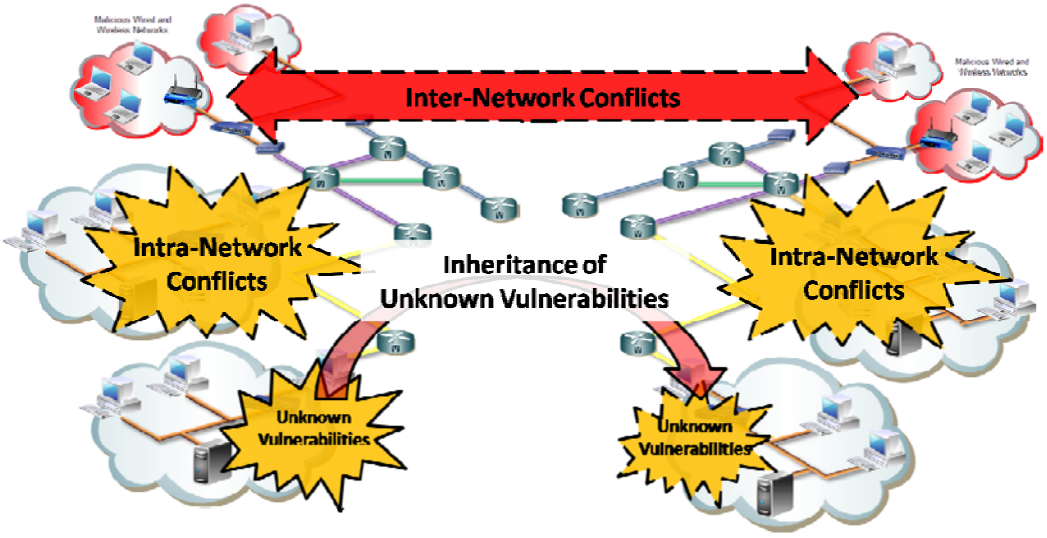


Figure 5. System-level Vulnerabilities

Within a standalone network, security research works [12] highlight the daunting task of configuring network security policies to govern network devices. The task remains complex and error-prone because of the rule dependency semantics and policy interaction in the network. The taxonomy of policy conflicts includes intra-policy and inter-policy conflicts. The intra-policy conflicts were summarized in the categories highlighted as follows:

1. Shadowing – A rule is shadowed when data packets match some other preceding rules that call for the execution of a very different set of actions, instead of the one crafted by the “shadowed” rule.

2. Correlation – This conflict is created when data packets match two rules, and the set of actions to take will be dependent on the ordering of these rules, which may not served the intended purpose correctly.

3. Exception – Conflicts are generated as a result when a matching rule is a subset of another rule, where the latter has a different set of actions for the data packets.

4. Redundancy – A rule is redundant when data packets match a rule that has similar set of actions as specified by another rule.

As presented in [12], the Inter-policy conflicts are categorized into two areas, namely “shadowing” and “spuriousness.” While shadowing conflicts are similar to that described in intra-policy conflicts, conflicts generated in the category of “spuriousness” give rise to a situation where data packets are permitted by a upstream policy but blocked by a downstream policy.

System-level vulnerabilities that are aggregated as a result of integrating large networks is a complex issue. It is also a relatively new area of research to address these system-level vulnerabilities, because not many open source publications are available for review. As such, it seemed logical to start extrapolating the concept of security policy conflicts from a single network perspective to one that encompasses a larger scope, as highlighted in Figure 5. Using it as a framework to understand the types of vulnerabilities generated from intra-network and inter-network conflicts, a vulnerability assessment methodology can be developed to address these vulnerabilities at the system level.

With the current tools and techniques reviewed in the areas of network exploration, detecting authorized host and router connections, and vulnerability assessment, the next chapter will describe the proposed integrated approach model that will combine these “black-box” and “white-box” analysis tools and techniques in the context of detecting unauthorized connections by insider threats.

THIS PAGE INTENTIONALLY LEFT BLANK

III. AN INTEGRATED DETECTION MODEL

A. PROLOGUE

This chapter presents the design of an integrated analysis model that combines both “black-box” and “white-box” approaches to conduct network exploration and vulnerability assessment in the context of detecting unauthorized host and router connections in the network infrastructure of a target system-of-systems.

B. OVERVIEW

1. Recap of Problem Statement

As military operations increasingly integrate large system-of-systems to develop cutting-edge operational capabilities, it will become more challenging to assess the overall security posture of the composite system-of-systems. New vulnerabilities may be introduced and insider threats may exploit these to establish unauthorized host and router connections.

2. Strategy and Proposed Approach

The proposed strategy is to leverage the complementary nature of “black-box” and “white-box” analysis approaches to improve current detection capabilities and enhance the network integrity of large integrated systems-of-systems. Key to the approach is a model to describe the structured process of a network exploration methodology. This methodology will prescribe how a network topology representation of a large integrated system-of-systems is mapped-out. Based on the network topology, the model will differentiate unauthorized connections from the legitimate ones. It will also conduct an integrated vulnerability assessment to determine the overall security posture and security impact of such unauthorized connections on the modeled large system-of-systems.

3. Assumptions

The methodology makes several assumptions regarding the networks to which the model will be applied. These include:

a. There is no prior knowledge regarding the network topology. As such, the methodology is applicable to almost all scenarios. This is also to prevent outdated network information from potentially corrupting the network exploration process in the model.

b. There exists a process (either via a trusted Network Administrator, databases, or the use of anomaly detection techniques) to determine off-line whether a given host, networking device, or network connection is authorized.

4. Model Overview

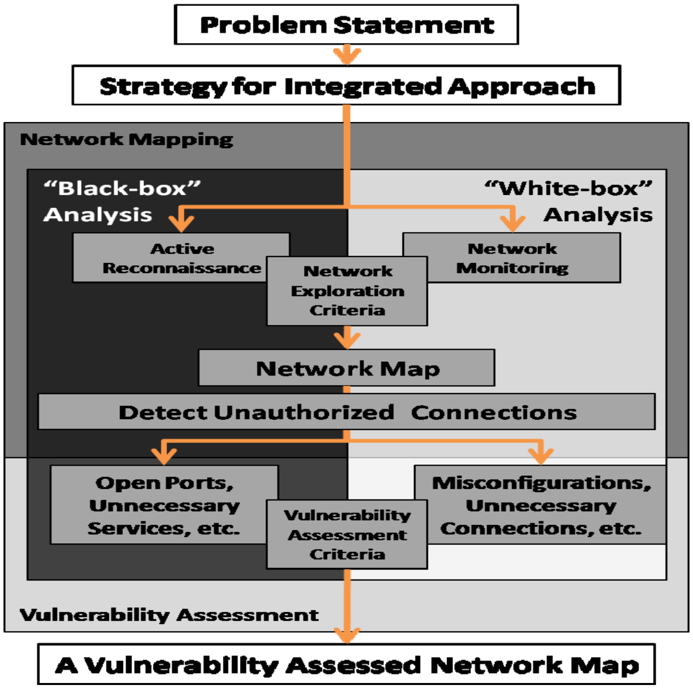

Problem Statement
Strategy for Integrated Approach
Network Mapping
"Black-box" Analysis
"White-box" Analysis
Active Reconnaissance
Network Exploration Criteria
Network Monitoring
Network Map
Detect Unauthorized Connections
Open Ports, Unnecessary Services, etc.
Vulnerability Assessment Criteria
Misconfigurations, Unnecessary Connections, etc.
Vulnerability Assessment
A Vulnerability Assessed Network Map

Figure 6. Integrated Analysis Model

The analytical model, as shown in Figure 6, applies a structured approach to develop an integrated network exploration and vulnerability assessment methodology. The methodology is geared towards detecting unauthorized connections and providing a vulnerability-assessed network map as an output for evaluation, as described in the Chapter IV. With a set of predefined network exploration criteria that specifies the attributes of a network map, the model will adopt a modular approach to use relevant tools and techniques to combine “black-box” and “white-box” analyses. The modular approach provides flexibility in deciding which tools and techniques to use in the areas of active reconnaissance and network monitoring to conduct network mapping. It will also allow a network manager to keep the model current with the latest network exploration tools and techniques.

With the network map constructed and essential network information (such as host information and networking protocols) annotated in the network map, the model will generate a list of suspicious network connections for more refined analysis. It will establish a process to query an authoritative entity to verify the network information annotated on the network map, differentiating authorized from unauthorized hosts and networking devices. With the list verified, the model will monitor real-time changes to the network map and use anomaly-based detection techniques to monitor the traffic generated from this list. This is to highlight the unauthorized connections that can be attributed to insider attacks.

Upon detection of these unauthorized connections, the model will use a prescribed set of criteria to conduct vulnerability assessment of the integrated system-of-systems. It will continue the modular approach, selecting tools and techniques from “black-box” and “white-box” analysis approaches. The model will generate a series of vulnerabilities and categorize them into Intra-network and Inter-network vulnerabilities to provide a “first-cut” perspective of a holistic vulnerability assessment of the network. The model will take a step further to determine the impact of unauthorized connections on the integrity of the defended network, which can provide a refined resolution of the vulnerabilities. At the end of the modeling process, the model will produce a vulnerability-assessed network map of the defended network to aid the network monitoring functionalities of the network administrators and network security engineers.

C. AN INTEGRATED APPROACH TO NETWORK EXPLORATION

The model adopts an approach that integrates the strengths of “black-box” analysis and “white-box” analysis to conduct network exploration of the defended network. It involves identifying a set of network exploration criteria to determine the essential network information that the network map will display. It will also adopt a modular approach to select tools and techniques from the areas of Active Reconnaissance and Network Monitoring to provide essential network information from which to construct the network map. A correlation engine is used in the model to aid and validate the detection of unauthorized connections in the network map. The engine correlates the network information produced by each tool and technique, stores the correlated information in a database, and highlights those that have information disparity for further inspection.

1. Network Exploration Criteria

The set of network exploration criteria defines what network mapping capabilities the tools should have to build a network map. It also defines the type of network information that needs to be available on the network map to detect unauthorized connections and perform vulnerability assessment. The set of criteria identifies the metrics used to assess the completeness of the network map and its supportability for detecting unauthorized connections. The key consideration for developing the set of criteria is to have it focus on essential network information that will substantiate unauthorized connections, yet prevent the network map from being over-cluttered with unnecessary information when larger systems-of-systems are considered. The criteria are identified in Table 1.

S/No.	Criteria	Network Information
1.	Positive Identification of all available Host and Networking Devices	Physical Topology = (Hosts and Networking Devices, Edges); Device Name and IP Address for Each Host or Networking Device
2.	Correct Type Identification of Host and Network Device	Type = Unknown, Client, Server, Router, Switch or Firewall
3.	Accurate Confirmation of Host and Networking Device Status	Availability Status = Unknown, Online or Offline
4.	Correct Identification of Operating System Type and Version	OS = Windows XP Service Pack1, Ubuntu, IOS version 12.1, etc.
5.	Detection of Ports and Services	Port Number; Status = Active or Inactive
6.	Correct Inventory Accountability of Hosts and Networking Devices	Number of Physical Hosts and Networking Devices in Network
7.	Detection of Unauthorized Hosts, Networking Devices, or Connections	Security Status = Authorized or Unauthorized

Table 1. A Set of Defined Criteria for Modeling Network Exploration

2. Incorporating Modularity in Model Design

The model incorporates modularity to provide flexibility in design and support system extensions. As depicted in Figure 7, the model does not dictate a fixed set of tools or techniques to be used, but instead is designed to allow the latest network mapping tools and new techniques to be employed. This facilitates flexibility in building a comprehensive network map. Such a modular approach will also generate information disparities between each tool and technique, which is precisely what the model is intending to do. An example of such information disparity might be when two different network mapping tools have differing findings on a host- or set of host-to-networking device connections. Information disparity may be used to trigger alerts for further inspection of the network for unauthorized connections, as described in a later section.

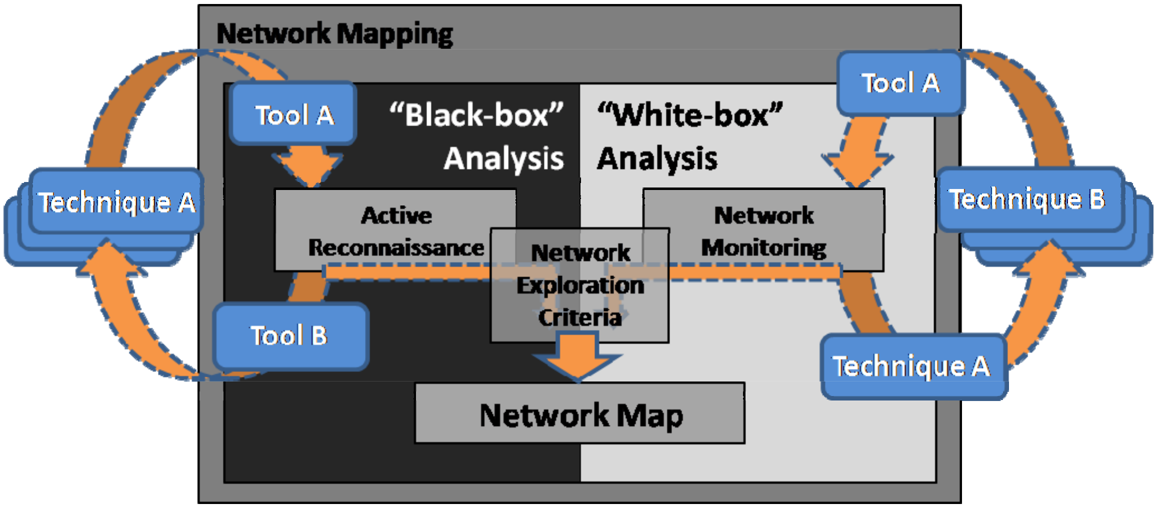


Figure 7. A Modular Design for Network Exploration

In the event there are information gaps in the network map that go beyond the capabilities of the currently employed tools and techniques, the network manager may bring in more advanced tools and techniques in the future as they become available. Regardless, these information gaps serve as useful feedback to form a data repository for network administrators and network security engineers to identify specifically what they do not know at that specific moment about their network. This is a key consideration because it is a challenging task to keep pace with the network topology as it is constantly evolving. Precise identification of such information gaps will aid the network administrators in planning protection measures against the vulnerabilities.

3. The Integrated Network Exploration

The integrated network exploration will employ active reconnaissance tools to conduct a preliminary scan of the defended network, followed by using network-monitoring techniques to elicit more network information from networking devices detected during the reconnaissance activity. From the active reconnaissance toolkit, the model will utilize various types of pings to scan the network. For example, Internet Control Message Protocol (ICMP) pings may be used to detect the presence of active hosts on the network. As most firewalls are configured to block ICMP packets, Simple Network Management Protocol (SNMP) pings may be used to check if there are any SNMP-enabled devices on the network, which can provide network information such as Domain Name Server (DNS) name, system names, system types, and system descriptions. In addition, TCP and User Datagram Protocol (UDP) pings may be used to determine if there are hosts that have their ports listening for connections, associated with well-known services (such as File Transfer Protocol (FTP), Secure Shell (SSH), Telnet, etc.). Since these techniques are only useful in detecting hosts and networking devices that provide responses, the network map is not complete as there may be hosts that may not reply to the pings.

Network monitoring tools and techniques are used to derive network information from hosts and networking devices that are configured not to response to scanning. Typically, more network information is obtainable from networking devices, such as routers and switches. Routers and switches keep a record (such as a routing table) of neighboring networking devices, including connected hosts, so they know to which networking devices or hosts it can route or forward the received data traffic. Information that is relevant to network exploration includes the network identification, the IP address of neighbors, and interfaces of a host or networking device. The integrated network exploration model will correlate these two sets of network information to produce a network map with essential network information.

4. Detection of Unauthorized Connections

With the network map constructed for the defended network, the model will examine the correlated network information to discover any information disparity produced using the different tools and techniques. These disparities refer to the form of conflicting information, including IP addresses and the number of hosts and networking devices on the network. These are useful indications regarding the false "positives" and false "negatives" generated by the integrated network exploration methodology. These may also be indications that unauthorized connections have been detected that require further verification.

The model will use the network map as a basis to track changes to the topology, especially the ones that are newly connected and those that generated suspicious network traffic. It will first treat these new connections as unauthorized connections and employ a pattern-matching technique to differentiate the legitimate connections from those that are newly connected or unauthorized. To augment the decision on connections that are unauthorized, additional measures can be used to detect malicious traffic generated from these connections. However, this will be in the realm of an Intrusion Detection System. The model will highlight these suspicious or unauthorized connections and present the conflicting network information in the network map.

D. VULNERABILITY ASSESSMENT

The approach to vulnerability assessment is similar to that of network exploration, whereby a suite of vulnerability assessment tools are selected based on their capabilities to determine network vulnerabilities. "Black-box" analysis tools such as Nessus, Retina and Core Impact provide comprehensive vulnerability assessment by scanning for known vulnerabilities on an unknown network. For example, Nessus uses a security vulnerability database and self-written trusted binaries and detection signatures to detect specific vulnerabilities. Core Impact provides comprehensive information gathering through automated network discovery to provide the scope of the defended network, validates newly discovered vulnerabilities, and presents a centralized view of the network security posture. The conceptual idea behind this is to combine the findings from each of these tools to paint a comprehensive vulnerability assessment for the large defended system-of-systems.

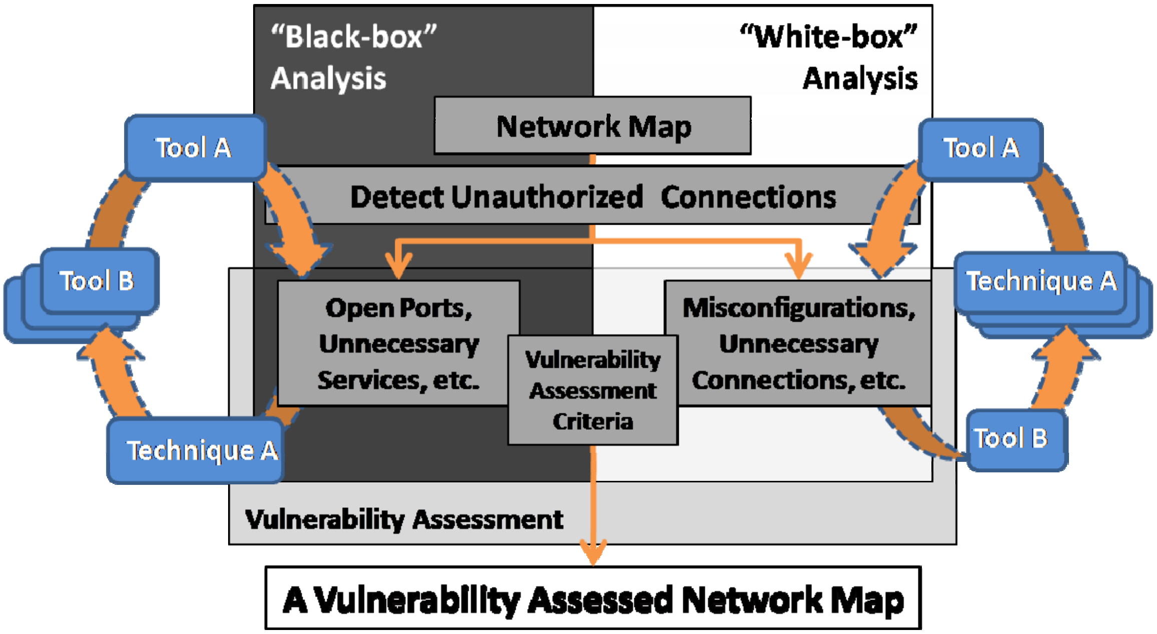

"Black-box" Analysis
"White-box" Analysis
Network Map
Detect Unauthorized Connections
Tool A
Tool B
Technique A
Tool A
Technique A
Tool B
Open Ports, Unnecessary Services, etc.
Vulnerability Assessment Criteria
Misconfigurations, Unnecessary Connections, etc.
Vulnerability Assessment
A Vulnerability Assessed Network Map

Figure 8. A Similar Modular Approach for Vulnerability Assessment

The model will combine the vulnerability assessment reports generated by the "black-box" analysis tools with the reports produced by "white-box" analysis tools such as Orion Network Configuration Management (NCM) and Nagios, as the latter focuses on network configurations and connectivity. The combined knowledge may generate some intuition on how vulnerabilities are generated at the system level when a complex system-of-systems is integrated. It will help to attribute the generation of these vulnerabilities to either intra-network conflicts or inter-network conflicts. Specifically, the model will use this integrated approach to assess the security impact of unauthorized connections to the network. It will conduct this integrated vulnerability assessment to differentiate the "new" vulnerabilities when such unauthorized connections are discovered.

In summary, the integrated approach to network exploration and vulnerability assessment aims at producing a network map that has been vulnerability-assessed using a combined suite of tools and techniques. As depicted in Figure 9, the generalized algorithm begins with a predefined set of criteria that defines the types of network information the tools and techniques should discover so that the network map will not be over-cluttered with unnecessary information for detecting unauthorized connections and vulnerability assessment. A set of network reconnaissance tools will be selected and for each tool, network exploration will be done on the network with the discovered network information stored in a network information database. When the list of network reconnaissance tools are exhausted, a list of network monitoring tools will similarly be used to determine if there is more network information that has yet to be discovered by the network reconnaissance tools. New network information will be updated in the database. A list of “white-box” analysis queries will be determined to provide in-depth analysis of the network by complementing the “black-box” analysis in discovering hosts and networking devices that were not previously discovered. These nodes include hosts and networking devices that are either trivially inactive or more sophisticated in nature, where they are deliberately configured not to respond to pings. This additional network information is updated in the database. Until such time when the “white-box” analysis queries are exhausted, the correlated network information is retrieved from the database to construct a network map and stored separately in another database.

In detecting unauthorized connections in the network, the constructed network map will be used to verify the list of hosts and networking devices that are detected by the integrated approach and are verified as authorized by the authoritative entity. In some situations, the network map is expected to contain more network information than what the authoritative entity may know, which are the authorized list of nodes, but he may not know what is actually deployed. Upon correlating the network map with the added information on the list of authorized nodes provided by the authoritative entity, the network map is used by the network administrators and security managers to monitor the network by tracking newly connected hosts and networking devices for unauthorized activities. Once suspicious activities are detected, these new connections will be flagged as “suspicious”, from which the network administrators and security managers can further ascertain the vulnerabilities these suspicious connections introduced to the defended network.

To determine the vulnerabilities introduced by suspicious connections, a list of “black-box” vulnerability assessment tools will be employed, followed by a series of “white-box” analysis queries to confirm the presence of additional vulnerabilities generated by these unauthorized connections. These newly discovered vulnerabilities will be stored in a vulnerability database as they serve as good reference for responsive recovery actions, which is outside the scope of this thesis.

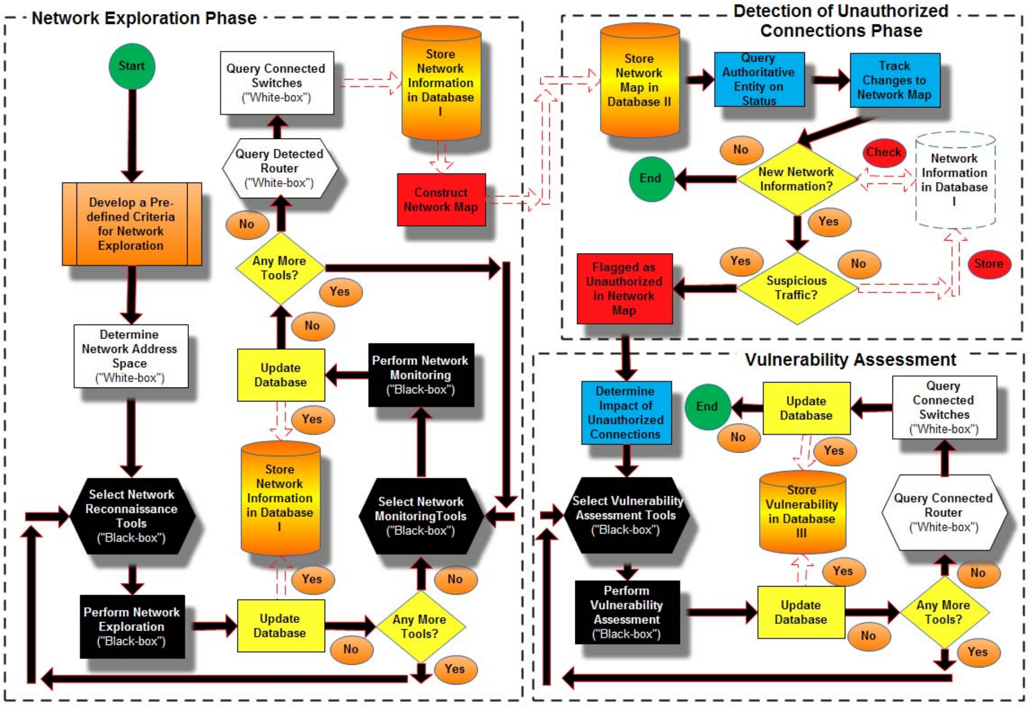

Network Exploration Phase
Start
Develop a Pre-defined Criteria for Network Exploration
Determine Network Address Space ("White-box")
Select Network Reconnaissance Tools ("Black-box")
Perform Network Exploration ("Black-box")
Update Database
Yes
Store Network Information in Database I
Update Database
No
Any More Tools?
Yes
Select Network MonitoringTools ("Black-box")
No
Perform Network Monitoring ("Black-box")
Update Database
Yes
No
Any More Tools?
Yes
No
Query Detected Router ("White-box")
Query Connected Switches ("White-box")
Store Network Information in Database I
Construct Network Map
Detection of Unauthorized Connections Phase
Store Network Map in Database II
Query Authoritative Entity on Status
Track Changes to Network Map
No
End
New Network Information?
Check
Network Information in Database I
Yes
Yes
Suspicious Traffic?
No
Store
Flagged as Unauthorized in Network Map
Vulnerability Assessment
Determine Impact of Unauthorized Connections
End
No
Update Database
Yes
Query Connected Switches ("White-box")
Select Vulnerability Assessment Tools ("Black-box")
Store Vulnerability in Database III
Query Connected Router ("White-box")
Yes
No
Perform Vulnerability Assessment ("Black-box")
Update Database
No
Any More Tools?
Yes

Figure 9. Generalized Algorithm for the Integrated Approach

With the integrated detection model developed, the next chapter discusses the results of implementing the algorithm, as described in Figure 9, on a test-bed to evaluate its effectiveness to conduct network exploration, detect unauthorized connections, and conduct vulnerability assessment.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTING AND EVALUATION

A. PROLOGUE

This chapter describes the testing and evaluation of the integrated model introduced in the previous chapter for detecting unauthorized connections in networks. It documents the effort to implement the integrated model on a test bed and test its effectiveness in mapping the network, detecting unauthorized connections, and assessing the impact of such connections on network vulnerabilities. The evaluation is based on the comprehensiveness of the network information attainable from the test-bed according to the pre-defined set of criteria discussed in the previous chapter. The findings are compared against those achievable by current tools and techniques with the integrated “black-box” and “white-box” analysis approaches taken by the model to illustrate the security benefits of a combined approach.

B. LAYING THE “GROUND WORK”

A small network of systems is set up as a test-bed to implement and experiment with the integrated model for network exploration and vulnerability assessment. As depicted in Figure 10, the test-bed consists of a set of authorized hosts, servers and routers, and the network backbone to represent a network environment accessible through switch ports. Insider threats are simulated to have breached the physical security access and able to establish unauthorized network connections in the form of rogue host computers, routers, or wireless access points. These connections will be malicious in nature as they will be used to launch attacks that range from sniffing confidential information from the network, to generating large network traffic for denial of service attacks against legitimate users.

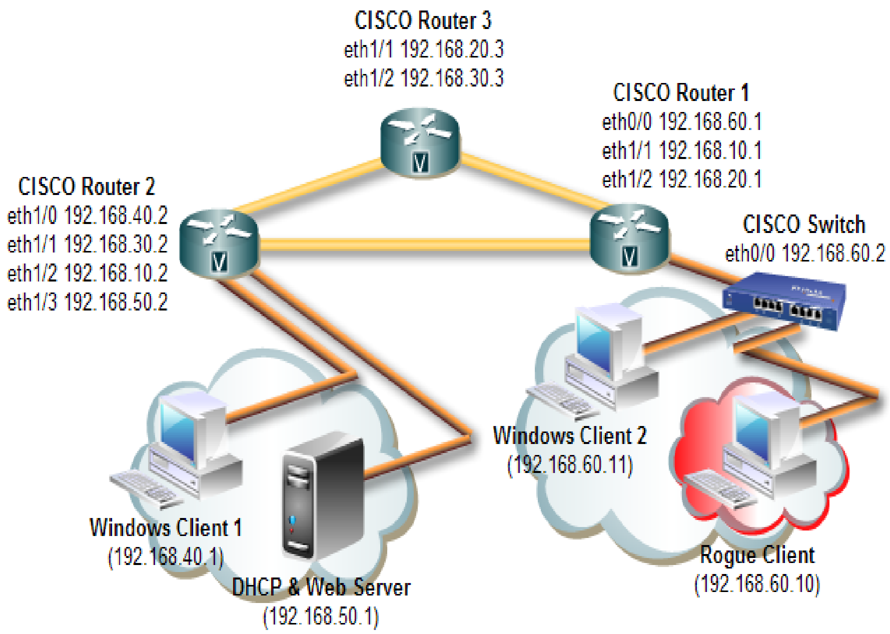


Figure 10. A Simple Test Bed

C. IMPLEMENT INTEGRATED NETWORK EXPLORATION

The integrated model for network exploration and vulnerability assessment, as defined in Chapter III, is implemented as an algorithm that combines “black-box” and “white-box” tools and techniques. The collection of network information derived by the algorithm, and other key parameters, is defined as follows:

Network Topology detectable by “Black-box” Analysis = (V_b, E_b)

Network Topology derivable by “White-box” Analysis = (V_w, E_w)

Authorized Topology G = (V, E)

Actual Topology G’ = (V’, E’);

where the first element of a tuple (e.g., V_b or V_w) represents the set of hosts and networking devices, and the second element the set of edges in the network.

The algorithm is designed to attain as much network information as possible from the test-bed (*G’ = (V’, E’)*), using the set of pre-defined criteria to determine what to gather for constructing the network map. The goal is to achieve an exact representation of the actual hosts and networking devices operating within the test-bed. This optimality criterion for the algorithm can be simply represented by the following condition:

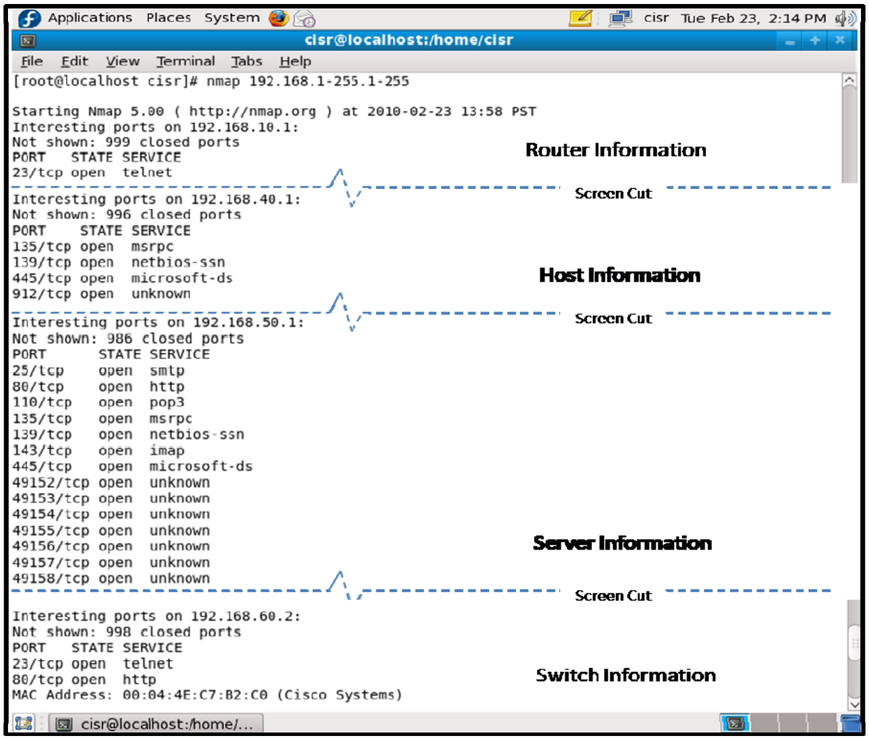
$$V_b \text{ U } V_w = V' \text{ and } E_b \text{ U } E_w = E' .$$

In general, the error of the algorithm can be modeled by a tuple variable Δ such that

$$\Delta = \{v_i,e_i| (v_i \in V' \wedge v_i \notin (V_B \cup V_W)) \vee (v_i \notin V' \wedge v_i \in (V_B \cup V_W)), (e_i \in E' \wedge e_i \notin (E_B \cup E_W)) \vee (e_i \notin E' \wedge e_i \in (E_B \cup E_W)) \}.$$

1. Conduct Network Reconnaissance

With the assumption that the algorithm has no prior network information regarding the test-bed, the “black-box” analysis tools and techniques are employed to provide a baseline network topology. This step, referred to as Network Reconnaissance, provides a quick first-cut view of hosts and networking devices operating on the network. These “live” nodes respond to the pings (traffic messages) sent out by the tools to elicit responses, and reply with their network information. Upon connection to the test-bed, the Dynamic Host Configuration Protocol (DHCP) configured for the network assigns an IP address to any new connection, and this IP address will determine the network address space in which pings can be launched to determine more network information, based on the set of pre-defined criteria that is needed to construct the network map. For example, if the DHCP client on the reconnaissance host receives the network address and mask 192.168.1.45/28, then the model launches the command ‘nmap 192.168.1.33-46. In the test, the reconnaissance host receives a 192.168.60.10, so the model launches Nmap, as depicted in Figure 11, to conduct a generic network scan to determine the number of “live” hosts on the network using the command “nmap 192.168.1-255.1-255”.

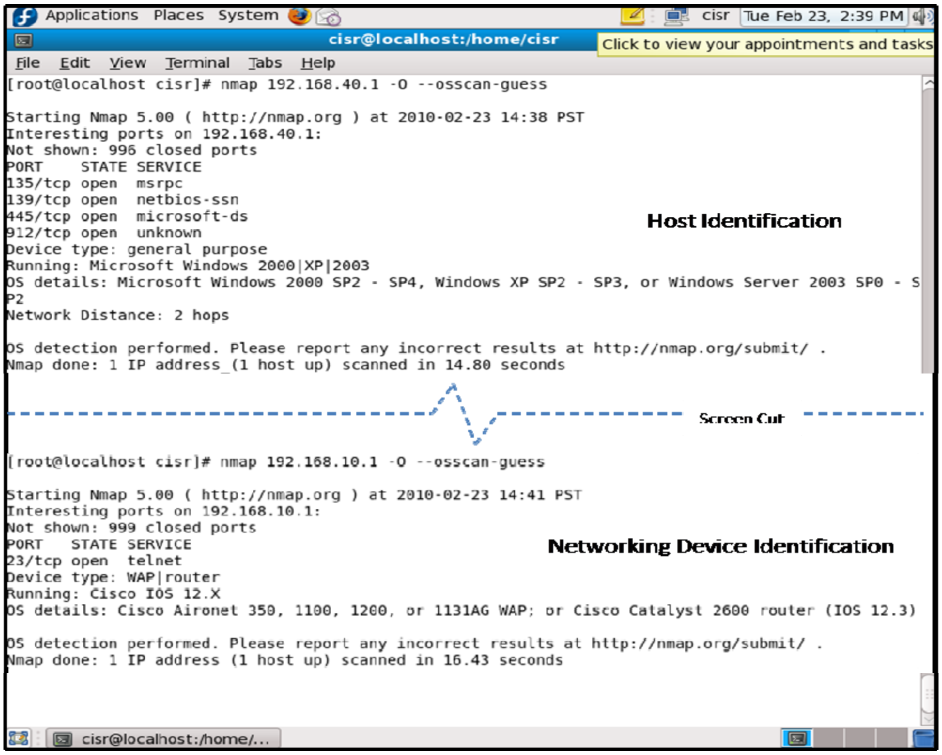


```
[root@localhost cisr]# nmap 192.168.1-255.1-255

Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-23 13:58 PST
Interesting ports on 192.168.10.1:
Not shown: 999 closed ports
PORT   STATE SERVICE
23/tcp open  telnet

Interesting ports on 192.168.40.1:
Not shown: 996 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
912/tcp open  unknown

Interesting ports on 192.168.50.1:
Not shown: 986 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown

Interesting ports on 192.168.60.2:
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:04:4E:C7:B2:C0 (Cisco Systems)
```

Figure 11. Network Information Generated from Nmap

The scan involves sending out ICMP Echo Request packets on the network and waiting for responses. Active hosts and networking devices that respond are then enumerated using “Synchronize (SYN) scans” on each of the TCP ports, 80 and 443, and are marked as “live” hosts on the network. Since ICMP pings are known to be blocked by patched systems, more advanced techniques, such as customizing TCP pings and ICMP messages, are needed to direct pings to specific well-known ports, such as Web servers (port 80), DHCP servers (port 67), and DNS servers (port 53) etc. Customizing these pings using commands like “nmap –sP –PS80 192.168.50.1/24” provide confidence that these ping packets are not dropped by firewalls protecting the hosts or servers.

The command-line switch “-O -osscan-guess” is used to determine the operating system of the “live” hosts. It is commonly used to ascertain the vulnerabilities of the “live” hosts, but in this case it will serve as a source of network information that characterizes each host and networking device on the test-bed, as illustrated in Figure 12.


Applications Places System
cisr Tue Feb 23, 2:39 PM
cisr@localhost:/home/cisr
Click to view your appointments and tasks
File Edit View Terminal Tabs Help
Host Identification
Screen Cut
Networking Device Identification
cisr@localhost:/home/...

```
[root@localhost cisr]# nmap 192.168.40.1 -O --osscan-guess

Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-23 14:38 PST
Interesting ports on 192.168.40.1:
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
912/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or Windows Server 2003 SP0 - S
P2
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.80 seconds
```

```
[root@localhost cisr]# nmap 192.168.10.1 -O --osscan-guess

Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-23 14:41 PST
Interesting ports on 192.168.10.1:
Not shown: 999 closed ports
PORT    STATE SERVICE
23/tcp open  telnet
Device type: WAP|router
Running: Cisco IOS 12.X
OS details: Cisco Aironet 350, 1100, 1200, or 1131AG WAP; or Cisco Catalyst 2600 router (IOS 12.3)

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.43 seconds
```

Figure 12. Detailed Identification Information Provided by Nmap

The proposed approach provides flexibility in the employment of network exploration tools (i.e. users can select other network exploration tools and/or techniques besides Nmap). This is to allow the network information attained by Nmap to be verified and validated by other tools within the integrated approach. The gathered network information will be stored in a data-structure, which will be used later to construct the network map of the test-bed.

2. Employ Network Monitoring Tools for Mapping

Network monitoring tools are employed, as they provide more comprehensive network information for known network devices to extend monitoring and management. Tools, such as LANsurveyor, provide network mapping capability to accomplish their primary function of network monitoring and management. This particular tool accomplishes this by providing a graphical display of the network information garnished by sending Simple Network Management Protocol (SNMP) and ICMP Pings to the hosts on the test-bed, as shown in Figure 13.

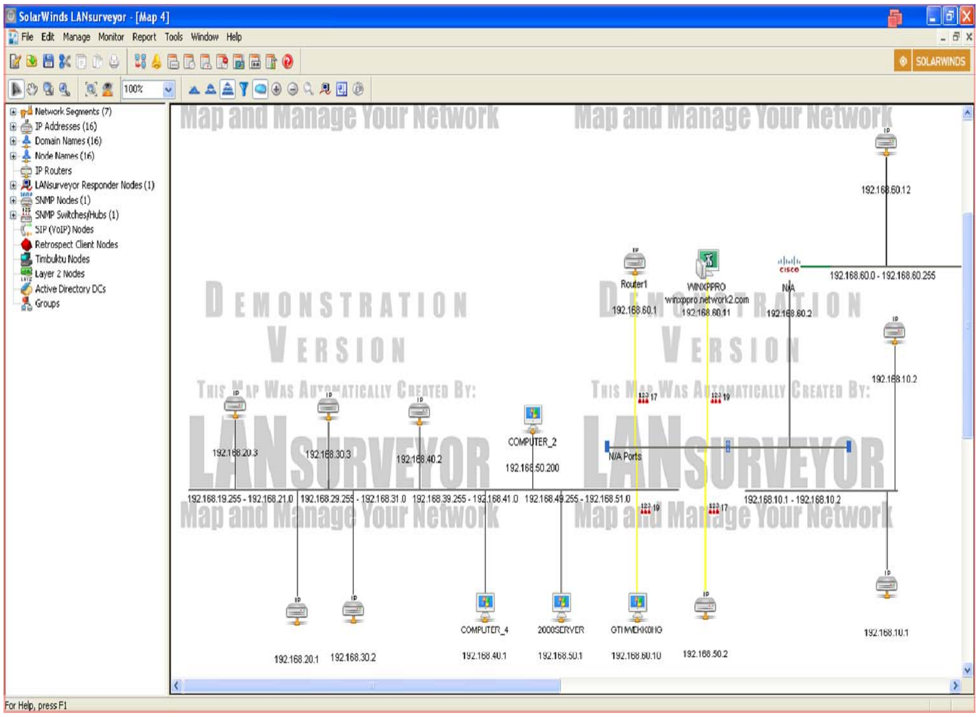
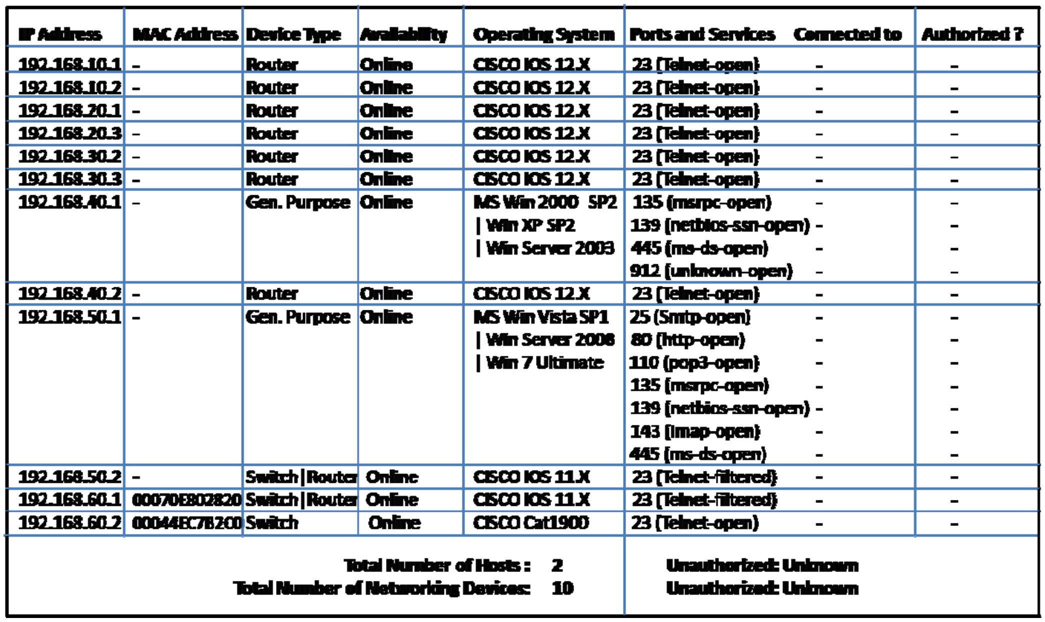


Figure 13. Network information from LANSurveyor

The network information generated by these tools is useful for verifying the efforts of network reconnaissance even though the tools are more time-consuming and not scalable for large networks, as compared to Network Reconnaissance tools. Table 2 provides a brief summary of what the “Black-box” analysis approach has gathered, with respect to the set of criteria defined in Chapter III for constructing the network map.



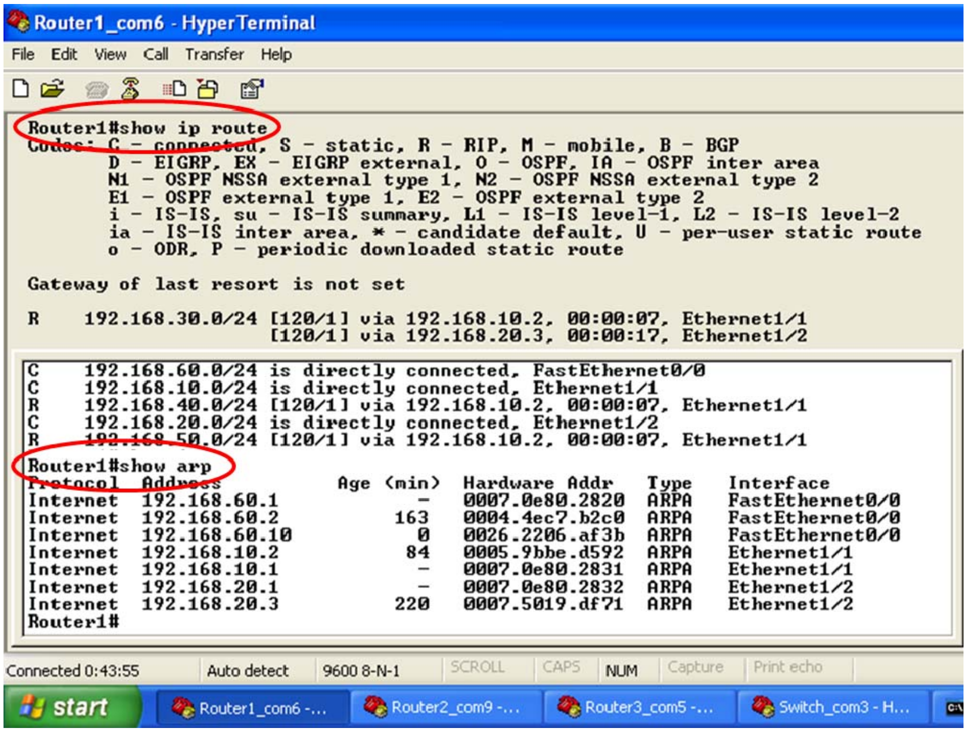
IP Address	MAC Address	Device Type	Availability	Operating System	Ports and Services	Connected to	Authorized ?
192.168.10.1	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.10.2	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.20.1	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.20.3	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.30.2	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.30.3	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.40.1	-	Gen. Purpose	Online	MS Win 2000 SP2 | Win XP SP2 | Win Server 2003	135 (msrpc-open) 139 (netbios-ssn-open) 445 (ms-ds-open) 912 (unknown-open)	- - - -	- - - -
192.168.40.2	-	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	-	-
192.168.50.1	-	Gen. Purpose	Online	MS Win Vista SP1 | Win Server 2008 | Win 7 Ultimate	25 (Smtp-open) 80 (http-open) 110 (pop3-open) 135 (msrpc-open) 139 (netbios-ssn-open) 143 (Imap-open) 445 (ms-ds-open)	- - - - - - -	- - - - - - -
192.168.50.2	-	Switch | Router	Online	CISCO IOS 11.X	23 (Telnet-filtered)	-	-
192.168.60.1	00070E802820	Switch | Router	Online	CISCO IOS 11.X	23 (Telnet-filtered)	-	-
192.168.60.2	00044EC7B200	Switch	Online	CISCO Cat1900	23 (Telnet-open)	-	-
				Total Number of Hosts : 2 Total Number of Networking Devices: 10	Unauthorized: Unknown Unauthorized: Unknown		

Table 2. Information Attained from “Black-box” Analysis

So far, the network information gathered by the “black-box” analysis approach, represented by *(V_b, E_b)*, are hosts and networking devices that are operating openly on the network. It is not complete because it does not include hosts or networking devices that are not active on the network at the time of the scan. It has no details of the MAC addresses that can be used to associate the detected IP addresses to the physical hosts or networking devices. There is also no information on the connected-ness of each detected device. This information is critical for a Nodal Dependency Study—one that analyzes the edge dependency of each node or networking device so that the cascading effect of a node failure can be studied in detail to assess the level of redundancy of crucial required network resources, and thereby the robustness of the network. It is important that the network map is complete, as an undetected host may not have been online during the network discovery process or may in fact be a malicious device that an insider threat deliberately configured to evade detection and sniff confidential data silently off the network. In this case, the authorization level of the undetected host or networking device is unknown.

3. Query the Edge Routers in the Network

A “white-box” analysis approach can gather network information about hosts that are not “live” on the network. This assumes that every connected host will have some form of signature or fingerprint captured in the form of a Media Access Control (MAC) address and an IP address. These information pieces are generally attainable from routers and switches deployed at the edge of the network, as they are essential for the routers and switches to either route or forward traffic from one host to another within the network. The process of gathering network information from these devices involves dedicated command-line queries for which the routers and switches are required to respond with information that contributes to the purpose of network exploration. As depicted in Figure 14, the CISCO commands “show ip route” and “show arp” are used to display IP routing table and the Address Resolution Protocol (ARP) table entries of the routers, respectively.

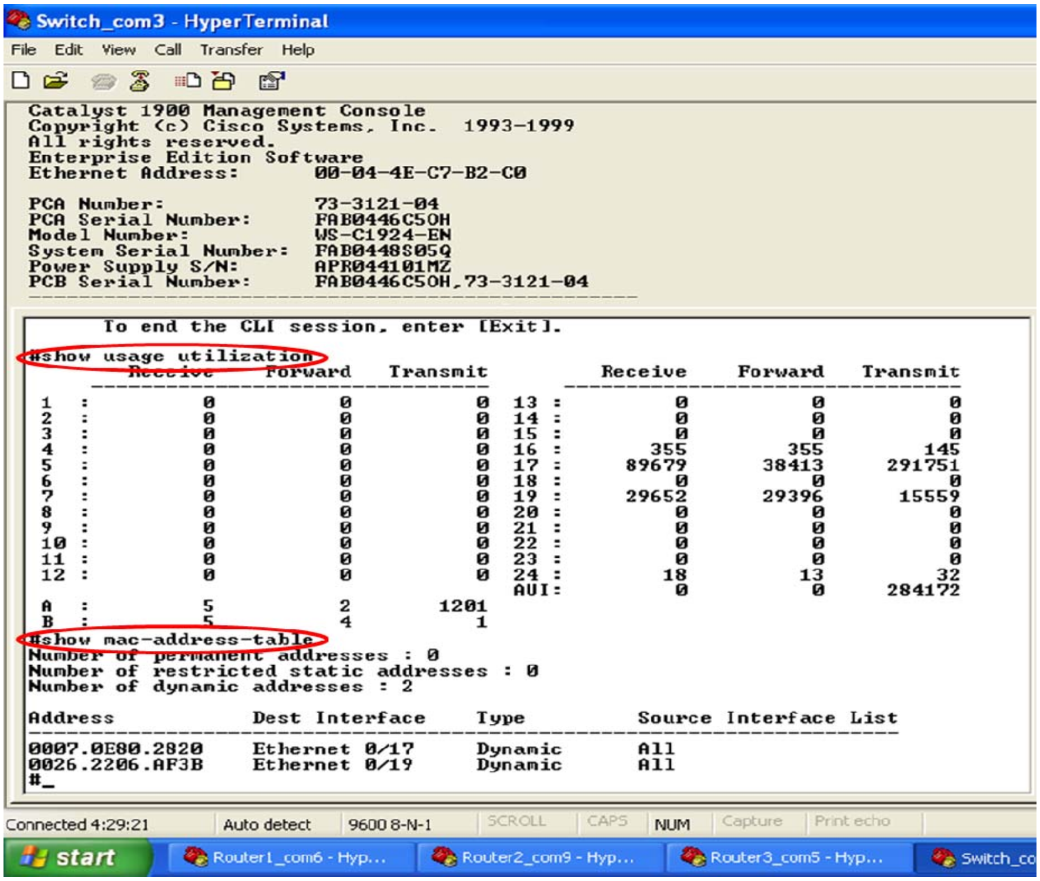


```
Router1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.30.0/24 [120/1] via 192.168.10.2, 00:00:07, Ethernet1/1
                     [120/1] via 192.168.20.3, 00:00:17, Ethernet1/2
C    192.168.60.0/24 is directly connected, FastEthernet0/0
C    192.168.10.0/24 is directly connected, Ethernet1/1
R    192.168.40.0/24 [120/1] via 192.168.10.2, 00:00:07, Ethernet1/1
C    192.168.20.0/24 is directly connected, Ethernet1/2
R    192.168.50.0/24 [120/1] via 192.168.10.2, 00:00:07, Ethernet1/1
Router1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.60.1            -   0007.0e80.2820  ARPA   FastEthernet0/0
Internet  192.168.60.2          163   0004.4ec7.b2c0  ARPA   FastEthernet0/0
Internet  192.168.60.10           0   0026.2206.af3b  ARPA   FastEthernet0/0
Internet  192.168.10.2           84   0005.9bbe.d592  ARPA   Ethernet1/1
Internet  192.168.10.1            -   0007.0e80.2831  ARPA   Ethernet1/1
Internet  192.168.20.1            -   0007.0e80.2832  ARPA   Ethernet1/2
Internet  192.168.20.3          220   0007.5019.df71  ARPA   Ethernet1/2
Router1#
```

Figure 14. Network Information Provided by Router

4. Query the Switches Connected to Edge Routers

As Layer-2 networking devices in the test-bed, switches provide the interface between routers and hosts that are connected to the network. They store useful network information about the connecting hosts so that they can forward the traffic data from the hosts to the routers, and vice versa. The network information useful for network exploration that can be gleaned from switches includes MAC addresses of all recently active connected hosts. The information gathering process involves using command-line queries such as “show usage utilization” and “show mac-address-table” to display the MAC addresses of the devices that are currently connected to the switch, and the utilization rate of each active port, respectively, as depicted in Figure 15.

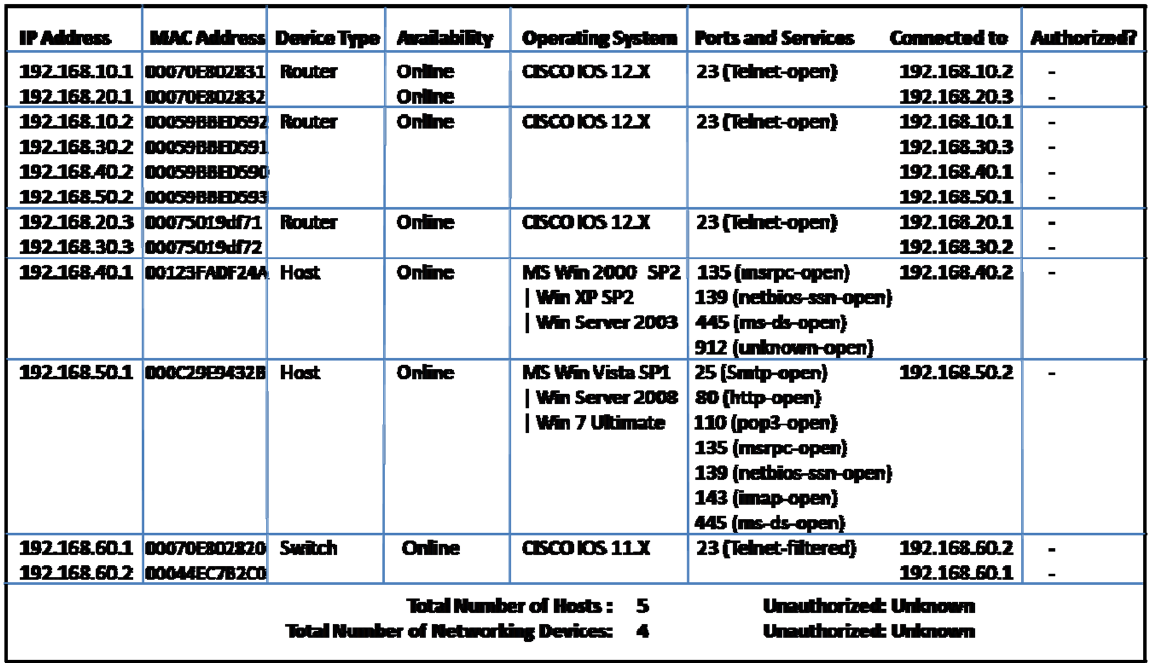


```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address:       00-04-4E-C7-B2-C0

PCA Number:             73-3121-04
PCA Serial Number:      FAB0446C50H
Model Number:           WS-C1924-EN
System Serial Number:   FAB0448S05Q
Power Supply S/N:       APR044101MZ
PCB Serial Number:      FAB0446C50H,73-3121-04
-------------------------------------------------------

        To end the CLI session, enter [Exit].

#show usage utilization
        Receive      Forward     Transmit            Receive     Forward    Transmit
      ------------------------------------       ------------------------------------
 1  :         0            0            0   13 :         0           0           0
 2  :         0            0            0   14 :         0           0           0
 3  :         0            0            0   15 :         0           0           0
 4  :         0            0            0   16 :       355         355         145
 5  :         0            0            0   17 :     89679       38413      291751
 6  :         0            0            0   18 :         0           0           0
 7  :         0            0            0   19 :     29652       29396       15559
 8  :         0            0            0   20 :         0           0           0
 9  :         0            0            0   21 :         0           0           0
 10 :         0            0            0   22 :         0           0           0
 11 :         0            0            0   23 :         0           0           0
 12 :         0            0            0   24 :        18          13          32
                                            AUI:         0           0      284172
 A  :         5            2         1201
 B  :         5            4            1
#show mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 2

Address             Dest Interface      Type            Source Interface List
-----------------------------------------------------------------------------
0007.0E80.2820      Ethernet 0/17       Dynamic         All
0026.2206.AF3B      Ethernet 0/19       Dynamic         All
#_
```

Figure 15. Network Information Provided by Switch

5. Construct the Network Map

By combining the network information from both the “black-box” and “white-box” analysis approaches, the network information gathered about the test-bed, represented by *(V_b U V_w , E_b U E_w),* is complete. In this scenario, the information is perfect (i.e., ∆ = empty) as highlighted in Table 3.

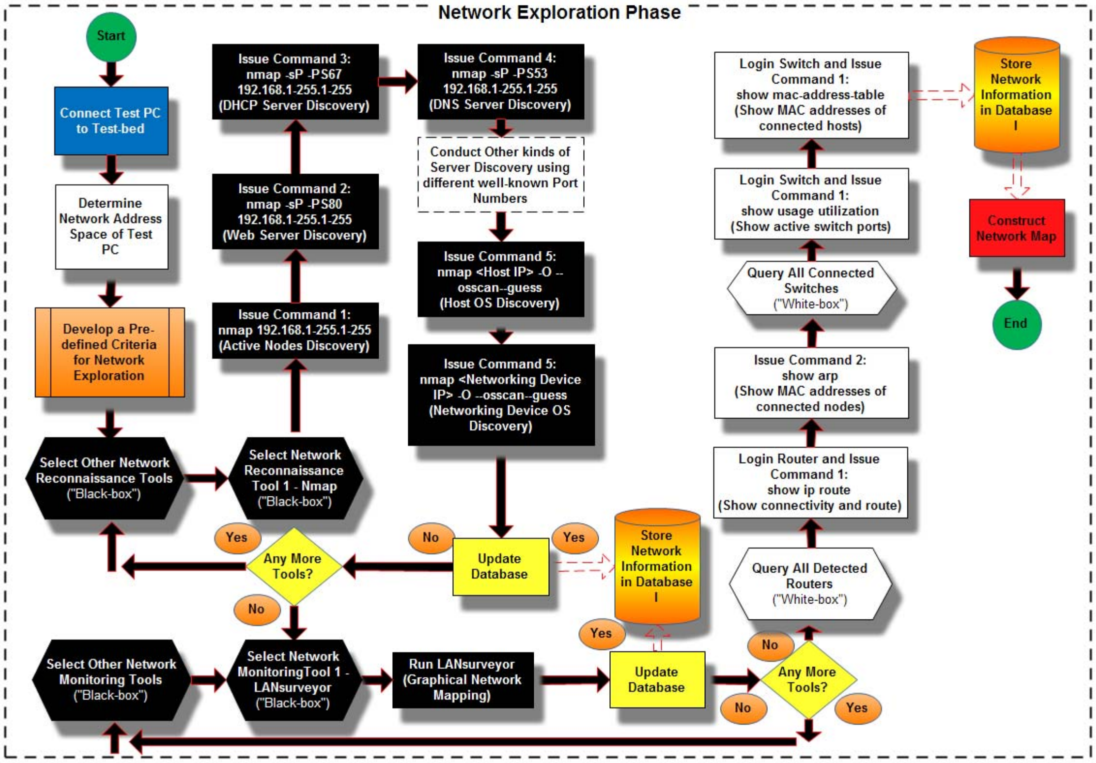


IP Address	MAC Address	Device Type	Availability	Operating System	Ports and Services	Connected to	Authorized?
192.168.10.1 192.168.20.1	00070E802831 00070E802832	Router	Online Online	CISCO IOS 12.X	23 (Telnet-open)	192.168.10.2 192.168.20.3	- -
192.168.10.2 192.168.30.2 192.168.40.2 192.168.50.2	00059BBED592 00059BBED591 00059BBED590 00059BBED593	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	192.168.10.1 192.168.30.3 192.168.40.1 192.168.50.1	- - - -
192.168.20.3 192.168.30.3	00075019df71 00075019df72	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	192.168.20.1 192.168.30.2	- -
192.168.40.1	00123FADF24A	Host	Online	MS Win 2000 SP2 | Win XP SP2 | Win Server 2003	135 (msrpc-open) 139 (netbios-ssn-open) 445 (ms-ds-open) 912 (unknown-open)	192.168.40.2	-
192.168.50.1	000C29E9432B	Host	Online	MS Win Vista SP1 | Win Server 2008 | Win 7 Ultimate	25 (Smtp-open) 80 (http-open) 110 (pop3-open) 135 (msrpc-open) 139 (netbios-ssn-open) 143 (imap-open) 445 (ms-ds-open)	192.168.50.2	-
192.168.60.1 192.168.60.2	00070E802820 00044EC7B2C0	Switch	Online	CISCO IOS 11.X	23 (Telnet-filtered)	192.168.60.2 192.168.60.1	- -
				Total Number of Hosts : 5 Total Number of Networking Devices: 4		Unauthorized: Unknown Unauthorized: Unknown	

Table 3. Combined Network Information Produced by Integrated Approach

With the integrated approach, more network information data points are correlated and provide a more coherent network topology of the test-bed. IP addresses detected by the “Black-box” analysis tools for the same router with different network interfaces can be correlated based on the detailed verification by the “White-box” analysis approach. MAC addresses collected from querying each router provides coherent network information that points to the different MAC addresses of the network interfaces of a given router. The immediate neighbor of each networking device can be determined based on the network hop information using “black-box” analysis that is verified by the “white-box” analysis approach. This information is useful for building a network map, similar to Figure 9, to be used to query an authoritative entity (either a trusted Networked Systems Architect or Chief Network Administrator) to determine the list of authorized hosts and networking devices, represented by *(V, E)*. This will support determination of disparities (i.e. $V_b \cup V_w - V$ *and* $E_b \cup E_w - E$) that are used to detect the unauthorized devices.

To summarize the efforts of combining “Black-box” and “White-box” analysis approaches, the algorithm to perform integrated network exploration of the test-bed is illustrated in Figure 16.



Network Exploration Phase
Start
Connect Test PC to Test-bed
Determine Network Address Space of Test PC
Develop a Pre-defined Criteria for Network Exploration
Select Other Network Reconnaissance Tools ("Black-box")
Select Network Reconnaissance Tool 1 - Nmap ("Black-box")
Issue Command 1: nmap 192.168.1-255.1-255 (Active Nodes Discovery)
Issue Command 2: nmap -sP -PS80 192.168.1-255.1-255 (Web Server Discovery)
Issue Command 3: nmap -sP -PS67 192.168.1-255.1-255 (DHCP Server Discovery)
Issue Command 4: nmap -sP -PS53 192.168.1-255.1-255 (DNS Server Discovery)
Conduct Other kinds of Server Discovery using different well-known Port Numbers
Issue Command 5: nmap <Host IP> -O --osscan--guess (Host OS Discovery)
Issue Command 5: nmap <Networking Device IP> -O --osscan--guess (Networking Device OS Discovery)
Update Database
No
Yes
Any More Tools?
Yes
No
Store Network Information in Database I
Select Other Network Monitoring Tools ("Black-box")
Select Network MonitoringTool 1 - LANsurveyor ("Black-box")
Run LANsurveyor (Graphical Network Mapping)
Update Database
Yes
Store Network Information in Database I
Any More Tools?
No
No
Yes
Query All Detected Routers ("White-box")
Login Router and Issue Command 1: show ip route (Show connectivity and route)
Issue Command 2: show arp (Show MAC addresses of connected nodes)
Query All Connected Switches ("White-box")
Login Switch and Issue Command 1: show usage utilization (Show active switch ports)
Login Switch and Issue Command 1: show mac-address-table (Show MAC addresses of connected hosts)
Store Network Information in Database I
Construct Network Map
End

Figure 16. Algorithm for Integrated Network Exploration

D. DETECT UNAUTHORIZED CONNECTIONS

The combined network information gathered from “black-box” and “white-box” analysis approaches will serve as a baseline state to address the specific problem of detecting unauthorized connections in the test-bed. A process is established whereby specific queries will be made to the authoritative entity to verify the list of authorized hosts and networking devices from the network map. The key to detecting unauthorized connections is the real-time correlation of new network information with that of the baseline state. A close monitoring capability of network anomalies generated from these correlations is necessary to ascertain if they are indeed unauthorized and malicious.

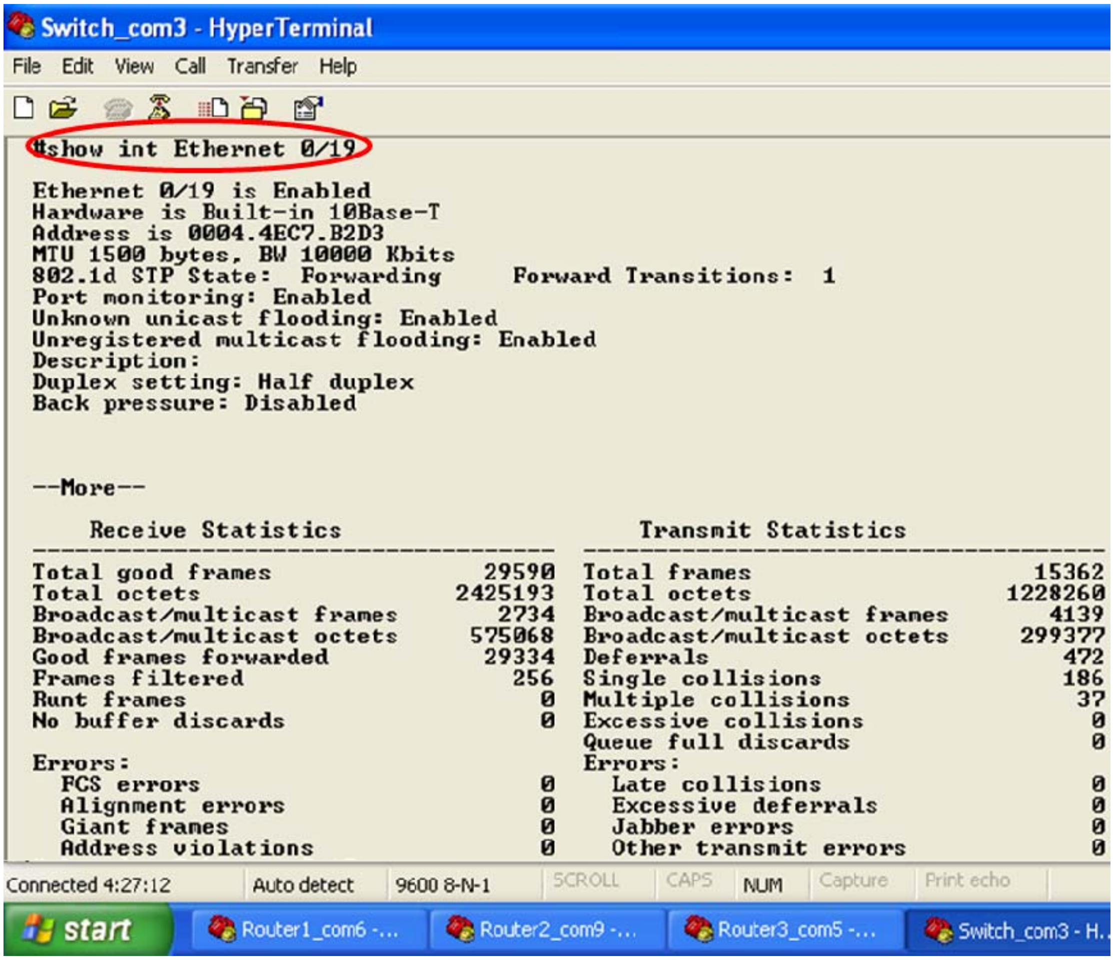
1. Correlate and Track Changes to Network Map

For the first test, a rogue host is connected to the switch to simulate that an unauthorized connection has been established. Attacks will be directed from this host to the network. It receives an assigned IP address of 192.168.60.10 from the DHCP Server, which is a new piece of network information that deviates from the network map generated according to the algorithm discussed in the previous sections. As part of the real-time correlation process, such information disparities and deviations from the network map are tracked closely. At this point, all new connections that are not part of the network (i.e. host connections with network information not captured in the network map) will be treated as suspicious and annotated in the network map. The integrated model will also adopt an anomaly-based detection technique to determine if the traffic generated from these connections is malicious in nature (i.e., characterized by either a sudden surge in large packet transfer from these connections into the network or large flow of traffic directed from the network to these connections).

2. Query Switch Ports Where Suspicious Hosts Are Connected

Upon detection of malicious traffic on the network generated from these new connections, the model will query the switch port to which the suspicious host is connected, so that its traffic is immediately tracked for anomalies. Querying the switch port using the command “show interface Ethernet 0/19” will display the traffic activities on Ethernet port 19 including the amount of traffic the connecting host has sent or received from the network, as depicted in Figure 17.

Malicious traffic generated from the unauthorized hosts or networking devices show a sudden surge in the total number of frames in the receive and transmit statistics, indicating that an attack has being initiated from this port.

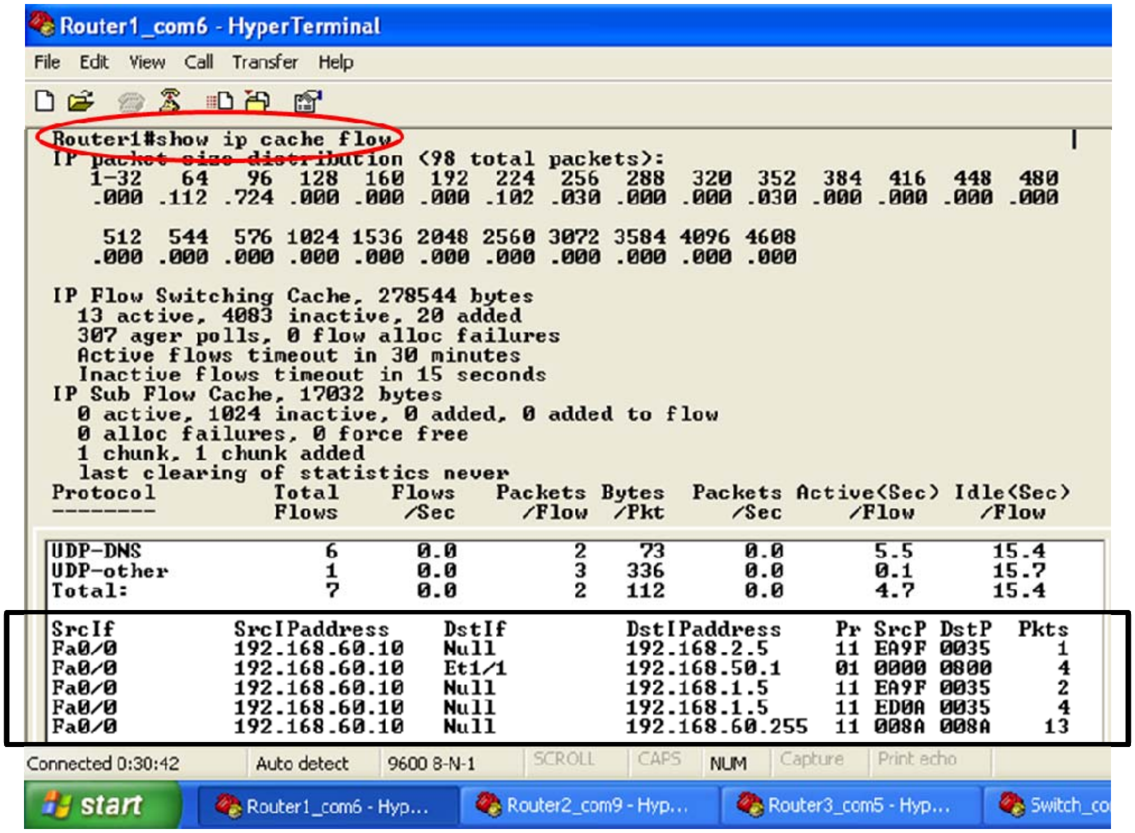


```
#show int Ethernet 0/19

 Ethernet 0/19 is Enabled
 Hardware is Built-in 10Base-T
 Address is 0004.4EC7.B2D3
 MTU 1500 bytes, BW 10000 Kbits
 802.1d STP State:  Forwarding     Forward Transitions:  1
 Port monitoring: Enabled
 Unknown unicast flooding: Enabled
 Unregistered multicast flooding: Enabled
 Description:
 Duplex setting: Half duplex
 Back pressure: Disabled


 --More--
     Receive Statistics                       Transmit Statistics
 -------------------------------------  -------------------------------------
 Total good frames              29590   Total frames                  15362
 Total octets                 2425193   Total octets                1228260
 Broadcast/multicast frames      2734   Broadcast/multicast frames     4139
 Broadcast/multicast octets    575068   Broadcast/multicast octets   299377
 Good frames forwarded          29334   Deferrals                       472
 Frames filtered                  256   Single collisions               186
 Runt frames                        0   Multiple collisions              37
 No buffer discards                 0   Excessive collisions              0
                                        Queue full discards               0
 Errors:                                Errors:
   FCS errors                       0     Late collisions                 0
   Alignment errors                 0     Excessive deferrals             0
   Giant frames                     0     Jabber errors                   0
   Address violations               0     Other transmit errors           0
```

Figure 17. Information on Traffic Generated by Suspicious Host

3. Employ NetFlow on Edge Router

For a more detailed analysis of the traffic generated from this switch port, network administrators may employ the NetFlow [15] functionality that is resident in Cisco routers and switches. Cisco embedded a network monitoring instrumentation, called NetFlow, to help network administrators understand the behavior of traffic flow in the network. In the test-bed, the router (with IP Address at 192.168.60.1) that is directly connected to the switch is configured to enable this functionality, This will generate a better understanding of the behavior of suspicious hosts connected to the switch.

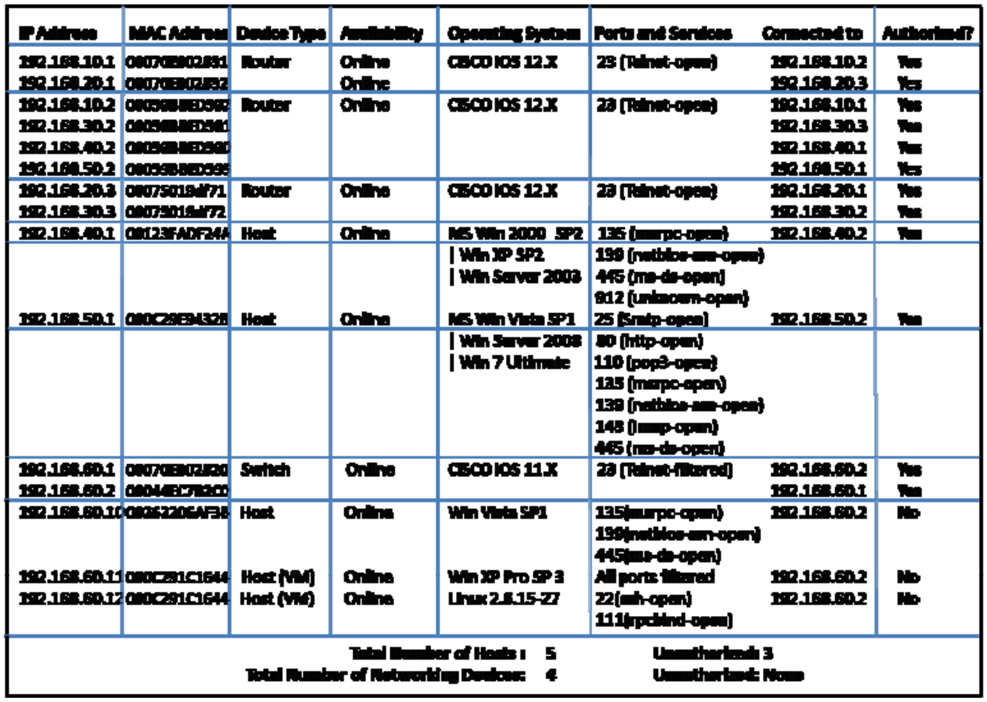

Router1_com6 - HyperTerminal
File Edit View Call Transfer Help

```
Router1#show ip cache flow
IP packet size distribution (98 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .112 .724 .000 .000 .000 .102 .030 .000 .000 .030 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  13 active, 4083 inactive, 20 added
  307 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17032 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

UDP-DNS              6      0.0         2    73      0.0       5.5      15.4
UDP-other            1      0.0         3   336      0.0       0.1      15.7
Total:               7      0.0         2   112      0.0       4.7      15.4

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0          192.168.60.10   Null           192.168.2.5     11 EA9F 0035     1
Fa0/0          192.168.60.10   Et1/1          192.168.50.1    01 0000 0800     4
Fa0/0          192.168.60.10   Null           192.168.1.5     11 EA9F 0035     2
Fa0/0          192.168.60.10   Null           192.168.1.5     11 ED0A 0035     4
Fa0/0          192.168.60.10   Null           192.168.60.255  11 008A 008A    13
```

Figure 18. Netflow Information on Unauthorized Connections

Upon receiving a stream of packets from the switch sent by a suspicious host, the router will examine the packets to look out for a set of IP packet attributes. It will then group the packets with similar attributes into a flow that will be stored in a cache in the NetFlow-enabled router. This network information can be retrieved to display the set of IP packet attributes; but more important is the information regarding the amount of traffic to which the tallied packets and bytes correspond. This is because attacks usually generate an unusually high amount of traffic to consume the network resources to cause denial-of-services. As shown in Figure 18, the command “show ip cache flow” is issued to display the amount of traffic generated and the corresponding destination IP addresses. It may also reveal if traffic is routed to a particular destination that is not cleared for hosts that are publicly connected via a switch port. Such information may be accumulated over time to identify the trend of attacks that do not occur immediately when the rouge device is connected.

To summarize, the efforts of combining “black-box” and “white-box” analysis approaches for the detection of unauthorized connections is shown to be possible with a simulated attack against the test-bed. The network information for the unauthorized connection is summarized in Table 4. In this case, the integrated approach revealed that there are three unauthorized hosts connected to the network, of which one had its ports filtered. They were detected as their corresponding MAC addresses and IP addresses differed from the original, baseline network map, which flagged them as “suspicious” connections, following which the confirmation of suspicious traffic flagged as “unauthorized” connections. The algorithm to perform the integrated approach to detecting unauthorized connections is illustrated in Figure 19.



IP Address	MAC Address	Device Type	Availability	Operating System	Ports and Services	Connected to	Authorized?
192.168.10.1 192.168.20.1	00070E802A31 00070E802A32	Router	Online Online	CISCO IOS 12.X	23 (Telnet-open)	192.168.10.2 192.168.20.3	Yes Yes
192.168.10.2 192.168.30.2 192.168.40.2 192.168.50.2	00059B8ED59E 00059B8ED591 00059B8ED590 00059B8ED595	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	192.168.10.1 192.168.30.3 192.168.40.1 192.168.50.1	Yes Yes Yes Yes
192.168.20.3 192.168.30.3	00075019df71 00075019df72	Router	Online	CISCO IOS 12.X	23 (Telnet-open)	192.168.20.1 192.168.30.2	Yes Yes
192.168.40.1	00123FADF24A	Host	Online	MS Win 2000 SP2	135 (msrpc-open)	192.168.40.2	Yes
192.168.50.1	000C29E94328	Host	Online	| Win XP SP2 | Win Server 2003 MS Win Vista SP1	139 (netbios-ssn-open) 445 (ms-ds-open) 912 (unknown-open) 25 (Smtp-open)	192.168.50.2	Yes
				| Win Server 2008 | Win 7 Ultimate	80 (http-open) 110 (pop3-open) 135 (msrpc-open) 139 (netbios-ssn-open) 143 (imap-open) 445 (ms-ds-open)		
192.168.60.1 192.168.60.2	00070E802A30 00044EC782C0	Switch	Online	CISCO IOS 11.X	23 (Telnet-filtered)	192.168.60.2 192.168.60.1	Yes Yes

192.168.60.10
192.168.60.11
192.168.60.12
	0026220GAF38
	000C291C1644
	000C291C1644
		Host
		Host (VM)
		Host (VM)
			Online
			Online
			Online
				Win Vista SP1
				Win XP Pro SP 3
				Linux 2.6.15-27
					135(msrpc-open)
					139(netbios-ssn-open)
					445(ms-ds-open)
					All ports filtered
					22(ssh-open)
					111(rpcbind-open)
						192.168.60.2
						192.168.60.2
						192.168.60.2
							No
							No
							No

				Total Number of Hosts : 5 Total Number of Networking Devices: 4		Unautherized: 3 Unautherized: None	

Table 4. Network Information On Unauthorized Connections

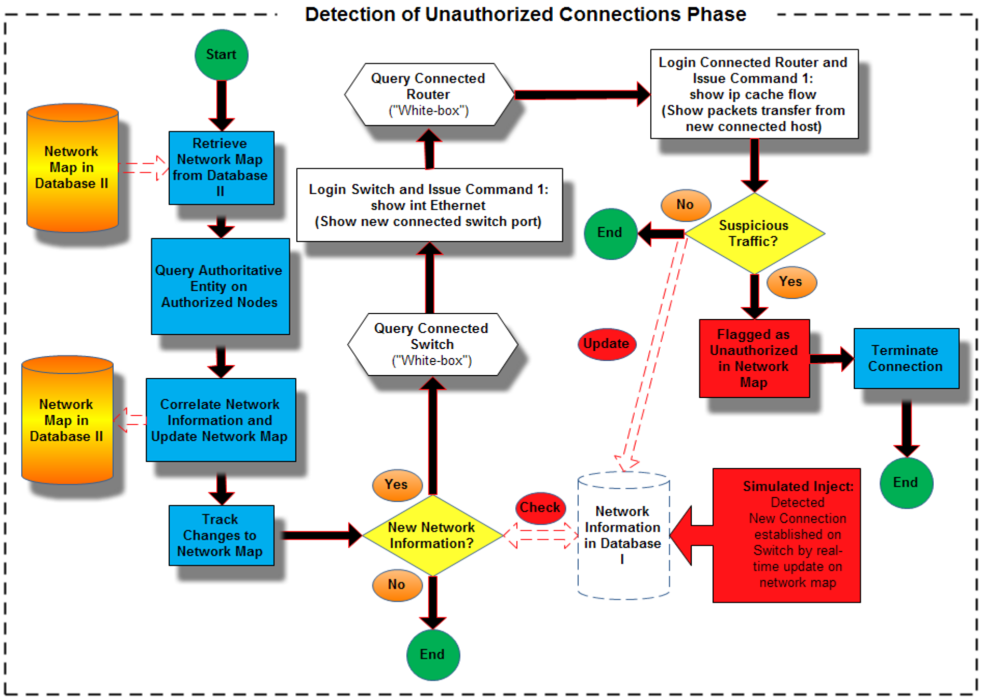

Detection of Unauthorized Connections Phase
Start
Network Map in Database II
Retrieve Network Map from Database II
Query Authoritative Entity on Authorized Nodes
Network Map in Database II
Correlate Network Information and Update Network Map
Track Changes to Network Map
Yes
New Network Information?
No
End
Query Connected Switch ("White-box")
Login Switch and Issue Command 1: show int Ethernet (Show new connected switch port)
Query Connected Router ("White-box")
Login Connected Router and Issue Command 1: show ip cache flow (Show packets transfer from new connected host)
No
End
Suspicious Traffic?
Yes
Update
Flagged as Unauthorized in Network Map
Terminate Connection
End
Check
Network Information in Database I
Simulated Inject: Detected New Connection established on Switch by real-time update on network map

Figure 19. Algorithm for Detecting Unauthorized Connections

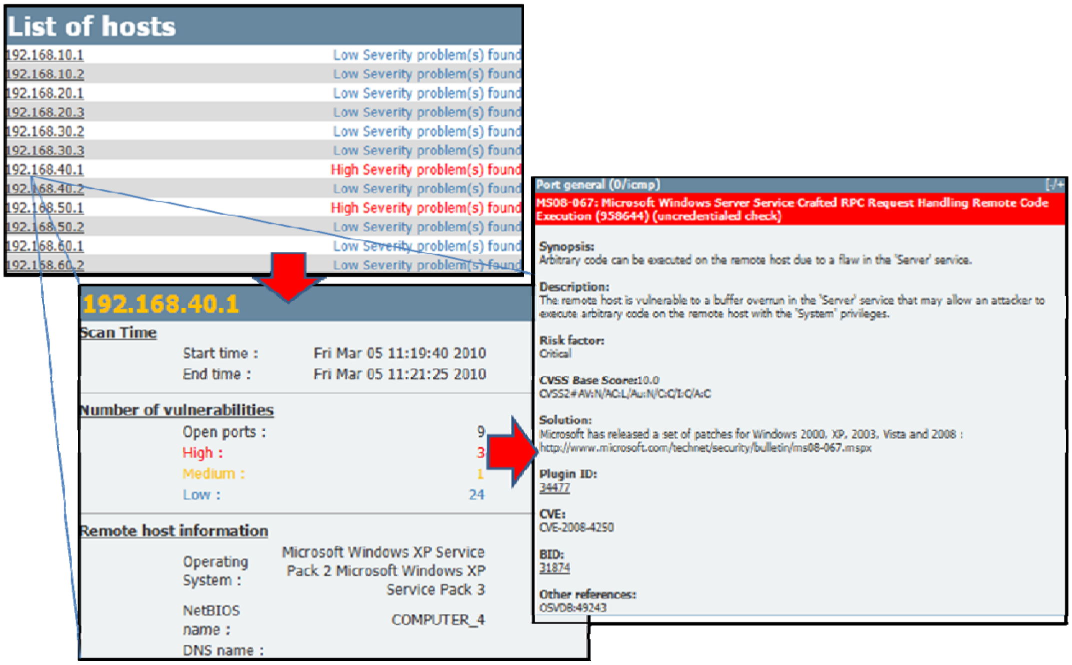
E. IMPLEMENT AN INTEGRATED VULNERABILITY ASSESSMENT

The integrated model employs a similar technique in performing vulnerability assessment on the test-bed. That is, it leverages various tools and techniques from “black-box” and “white-box” approaches to give a coherent vulnerability assessment of the network map generated for the test-bed.

1. Conduct Initial Intra-Network Vulnerability Assessment

When the network map is first developed it is important to conduct a vulnerability assessment to determine the network’s baseline vulnerabilities. These vulnerabilities are categorized as Intra-Network Vulnerabilities, and must be patched before integrating with other networked systems. Thereafter, with each networked system integrated, another vulnerability assessment must be done at the system-interface level (i.e. where these systems are integrated). In this test, an initial integrated vulnerability assessment was performed using

Nessus to detect vulnerabilities that can be exploited due to misconfigurations in the test-bed. The intra-network vulnerability assessment findings provided by Nessus are depicted in Figures 20. It provides an overview of the severity of the problems it has discovered for each host and networking device, and categorizes the vulnerabilities into three levels of severity. Nessus also provides a synopsis and the details of each vulnerability that are useful for network administrators to follow up and patch the system.



List of hosts

192.168.10.1	Low Severity problem(s) found
192.168.10.2	Low Severity problem(s) found
192.168.20.1	Low Severity problem(s) found
192.168.20.3	Low Severity problem(s) found
192.168.30.2	Low Severity problem(s) found
192.168.30.3	Low Severity problem(s) found
192.168.40.1	High Severity problem(s) found
192.168.40.2	Low Severity problem(s) found
192.168.50.1	High Severity problem(s) found
192.168.50.2	Low Severity problem(s) found
192.168.60.1	Low Severity problem(s) found
192.168.60.2	Low Severity problem(s) found

192.168.40.1

Scan Time

Start time : Fri Mar 05 11:19:40 2010
End time : Fri Mar 05 11:21:25 2010

Number of vulnerabilities

Open ports : 9
High : 3
Medium : 1
Low : 24

Remote host information

Operating System : Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3
NetBIOS name : COMPUTER_4
DNS name :

Port general (0/icmp) [-/+

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :
http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

Plugin ID:
34477

CVE:
CVE-2008-4250

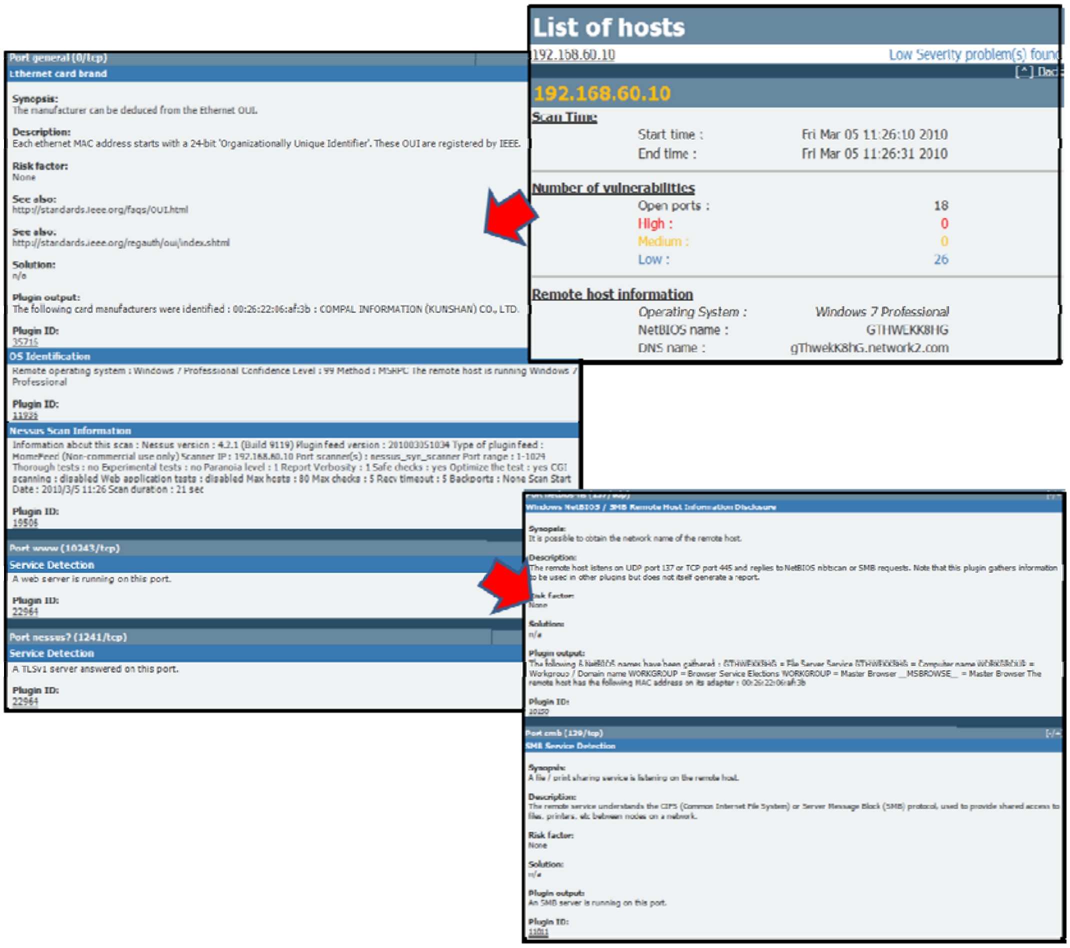
BID:
31874

Other references:
OSVDB:49243

Figure 20. Report Generated by Nessus

2. Determine Impact of Unauthorized Connections

Upon detection of unauthorized connections in the test-bed, the impact of these connections on the network must be determined. First, an assessment has to be performed on the detected unauthorized host or networking device as this will provide clues as to what vulnerabilities the unauthorized connections may introduce to the network. As depicted in Figure 21, Nessus is used to conduct a vulnerability assessment on the unauthorized host (with IP Address 192.168.60.10) that shows the severity level of each discovered vulnerability and the port information. The overall network integrity of the defended network is re-assessed to determine if such unauthorized connections have introduced more vulnerability in addition to what were previously patched in the initial assessment. Since Nessus provides a snapshot of the vulnerabilities, it discovered from the unauthorized connections that there is a need to query the connected router and switch to determine the activity level of the connections. The activity level, represented by the transmitted and received frames, will shed some light on whether new vulnerabilities are introduced. This is characterized by the sudden surge in data packets sent out from the connected switch and router. The algorithm for performing the integrated vulnerability assessment is illustrated in Figure 22.



Port general (0/tcp)

Ethernet card brand

Synopsis:
The manufacturer can be deduced from the Ethernet OUI.

Description:
Each ethernet MAC address starts with a 24-bit 'Organizationally Unique Identifier'. These OUI are registered by IEEE.

Risk factor:
None

See also:
http://standards.ieee.org/faqs/OUI.html

See also:
http://standards.ieee.org/regauth/oui/index.shtml

Solution:
n/a

Plugin output:
The following card manufacturers were identified : 00:26:22:06:af:3b : COMPAL INFORMATION (KUNSHAN) CO., LTD.

Plugin ID:
35716

OS Identification

Remote operating system : Windows 7 Professional Confidence Level : 99 Method : MSRPC The remote host is running Windows 7 Professional

Plugin ID:
11936

Nessus Scan Information

Information about this scan : Nessus version : 4.2.1 (Build 9119) Plugin feed version : 201003051034 Type of plugin feed : HomeFeed (Non-commercial use only) Scanner IP : 192.168.60.10 Port scanner(s) : nessus_syn_scanner Port range : 1-1024 Thorough tests : no Experimental tests : no Paranoia level : 1 Report Verbosity : 1 Safe checks : yes Optimize the test : yes CGI scanning : disabled Web application tests : disabled Max hosts : 80 Max checks : 5 Recv timeout : 5 Backports : None Scan Start Date : 2010/3/5 11:26 Scan duration : 21 sec

Plugin ID:
19506

Port www (10243/tcp)

Service Detection

A web server is running on this port.

Plugin ID:
22964

Port nessus? (1241/tcp)

Service Detection

A TLSv1 server answered on this port.

Plugin ID:
22964

List of hosts

192.168.60.10 Low Severity problem(s) found

[^] Back

192.168.60.10

Scan Time

Start time :	Fri Mar 05 11:26:10 2010
End time :	Fri Mar 05 11:26:31 2010

Number of vulnerabilities

Open ports :	18
High :	0
Medium :	0
Low :	26

Remote host information

Operating System :	*Windows 7 Professional*
NetBIOS name :	GTHWEKK8HG
DNS name :	gThwekK8hG.network2.com

Port netbios-ns (137/udp)

Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis:
It is possible to obtain the network name of the remote host.

Description:
The remote host listens on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins but does not itself generate a report.

Risk factor:
None

Solution:
n/a

Plugin output:
The following 6 NetBIOS names have been gathered : GTHWEKK8HG = File Server Service GTHWEKK8HG = Computer name WORKGROUP = Workgroup / Domain name WORKGROUP = Browser Service Elections WORKGROUP = Master Browser __MSBROWSE__ = Master Browser The remote host has the following MAC address on its adapter : 00:26:22:06:af:3b

Plugin ID:
10150

Port smb (139/tcp) [-/+]

SMB Service Detection

Synopsis:
A file / print sharing service is listening on the remote host.

Description:
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Risk factor:
None

Solution:
n/a

Plugin output:
An SMB server is running on this port.

Plugin ID:
11011

Figure 21. Vulnerability Assessment on Unauthorized Host

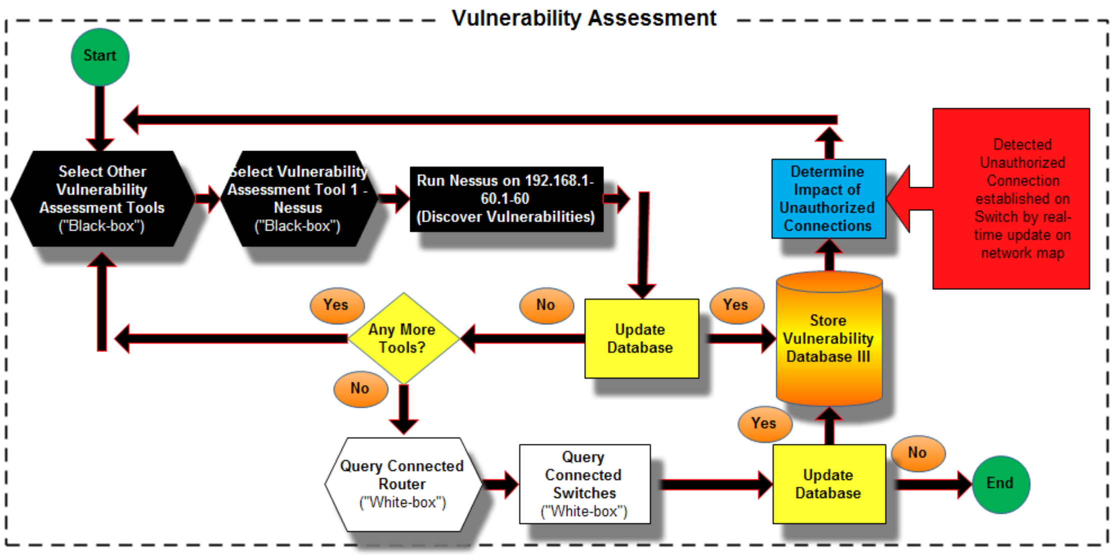

Vulnerability Assessment
Start
Select Other Vulnerability Assessment Tools ("Black-box")
Select Vulnerability Assessment Tool 1 - Nessus ("Black-box")
Run Nessus on 192.168.1-60.1-60 (Discover Vulnerabilities)
Determine Impact of Unauthorized Connections
Detected Unauthorized Connection established on Switch by real-time update on network map
Yes
Any More Tools?
No
Update Database
Yes
Store Vulnerability Database III
No
Yes
Query Connected Router ("White-box")
Query Connected Switches ("White-box")
Update Database
No
End

Figure 22. Algorithm for Vulnerability Assessment

3. Summary—An Algorithm for Integrated Approach

With the network map of the test-bed assessed by Nessus, the testing and evaluation of the integrated model was completed. In summary, the test-bed is successfully "explored" in the sense that a network map was generated with all connections, including the unauthorized connections. An initial vulnerability assessment was conducted to determine what needed to be patched before integration with other systems. The baseline network map was then used as a basis to detect unauthorized connections by detecting when changes were made to the topology. Upon detection of unauthorized connections, vulnerabilities induced by such connections were detected. With the vulnerability assessment completed, a vulnerability-assessed network map was generated, and was ready to be verified by an authoritative entity to confirm the findings of the integrated approach. Further security measures could then be taken by the system owners and network administrators to rectify the insider attacks.

The above implementation of the integrated model has demonstrated that there are high payoff areas in combining "black-box" and "white-box" analysis approaches in terms of network exploration, detecting unauthorized connections, and vulnerability assessment. The tests also showed that we can discover more network information and vulnerabilities using an integrated approach as compared to using such tools and techniques in isolation. The next chapter will conclude the findings of this thesis work and propose future work specifically in automating this integrated process with a program for network exploration and vulnerability assessment.

V. CONCLUSION AND RECOMMENDATIONS

A. PROLOGUE

This chapter concludes the thesis work by reviewing the research questions it was set out to achieve answering with its work. The integrated approach of combining “black-box” and “white-box” analysis for network exploration and vulnerability assessment established a strong, fundamental foundation to address the security issue of detecting unauthorized connections in a defended network. There is research space for strengthening the concept of an integrated approach, which will be discussed as future work as follow-on efforts to this thesis work.

B. CONCLUSION

The “black-box” and “white-box” analysis approaches were found to be complimentary for network exploration and vulnerability assessment. This is evident from the model design and experimental results from implementing the integrated model on the test bed. Two major observations supporting this conclusion are:

1. In the network exploration phase, the “black-box” analysis approach was able to map out hosts and networking devices that are active in the test bed. Examples of hosts and networking devices that are not detectable by the “black-box” analysis include those configured not to respond to pings, and those inactive but connected to the test bed. The “white-box” approach is complimentary to the “black-box” in the sense that it is able to query specific networking devices and traffic logs such as the Cisco NetFlow data to discover “inactive” hosts and networking devices. By issuing additional router or switch command line queries, such as “show interface,” “show ip route,” and “show arp,” one is able to the discover IP and MAC addresses of the hosts and networking devices not enumerated by the “black-box” analysis approach.

2. In detecting unauthorized connections, the “black-box” analysis approach can reveal specific IP addresses of suspicious hosts or networking devices by correlating network information. However, it cannot ascertain the nature of data traffic generated by these nodes, which is determining if the device activity is malicious. Nonetheless, these IP addresses served to guide the “white-box” analysis to query switches and routers connected to these suspicious nodes. Using the embedded NetFlow functionality in CISCO routers and switches, the command “show ip cache flow” displays the amount of data traffic generated from these suspicious nodes, which may be further analyzed to confirm that they are indeed unauthorized connections. Thus, the integrated approach paved a way to address the problem of detecting unauthorized connections in large operational networks.

This thesis work proposed a systematic way of combining “black-box” and “white-box” analysis approaches for network exploration and vulnerability assessment. It incorporates modularity in its design to leverage the strengths of open source tools and techniques to construct a network map to be used for detecting unauthorized connections, as confirmed either through off-line investigation or through an “intelligent oracle” that maintains the authorized topology, and assess the vulnerabilities that potentially may be introduced. Although not proven optimal, this systematic methodology demonstrated that there are high operational benefits garnered by combining the two analysis approaches. These include establishing a comprehensive network topology to serve as a baseline necessary to aid the network administrators and security managers, providing real-time detection of suspicious hosts and networking devices, and discovering potential vulnerabilities in the defended network.

C. RECOMMENDATIONS FOR FUTURE WORK

1. Automating the Integrated Model for Network Exploration and Vulnerability Assessment

This thesis work laid the steps by which the integrated model can be used for network exploration and vulnerability assessment, as shown in Figure 20. Using these steps to establish software requirements, follow-on work could develop an application program to automate these steps. Further, automation might be used to verify the methodology's capabilities to conduct network mapping, detect unauthorized connections on the network map, and determine the impact of unauthorized connections on the defended network. The program should also maintain currency with respect to integrating the latest tools and techniques available to probe or monitor networks, thereby constantly improving its capability in detecting unauthorized connections.

2. Evaluation of Algorithm on Large Operational Networks

This thesis effort focused on developing an analytical approach to evaluate the effectiveness of the integrated approach of combining "black-box" and "white-box" analysis in network exploration, detecting unauthorized connections, and vulnerability assessment in a simple test-bed. There is a need to extend the thesis work to evaluate the integrated model in large operational networks, verifying its effectiveness in network exploration and vulnerability assessment in such contexts. This will provide a practical and realistic approach to further validate the results and findings of this thesis work, providing more visibility of the operational benefits to be secured by deploying this integrated model in network operations centers.

3. In-depth Analysis on Detecting Unauthorized Connections

Another possible area of future work is to refine the process of discovering and further qualifying connections as unauthorized in the defended network. This can potentially take on the work of integrating an Intrusion Detection System (IDS) and embedding a behavior analysis capability into the model so that the integrated approach can evolve from a correlation engine to one that detects unauthorized connections primarily based on the behaviors of these connections. The enhanced system should be able to detect unauthorized connections even if these connections are camouflaged with spoofed IP and MAC addresses. It could also extend its detection of unauthorized wireless access points, which remains a challenging issue today. Addressing security issues related to network exploration and vulnerability assessment of an unknown wireless network environment will leapfrog the current research in securing wireless communications for both military and civilian applications.

4. Refining the Model Analysis Approach

This study sought to establish the potential utility of integrating black-box and white-box analysis techniques to detect unauthorized network connections. While this was accomplished, the methodology used a simple sequential application of the two techniques, similar to the classic “Waterfall” process of software engineering. However, as with managing software projects with less well understood requirements, a “spiral” methodology where iterative application of black-box and white-box techniques are applied to incrementally refine the network topology information may prove to hold benefit. When combined with automation of black-box and white-box tool application, a more thorough analysis of the network may be achieved.

LIST OF REFERENCES

[1] R. Gates, U.S. Defense Secretary (2009). Memorandum for Secretaries of the Military Departments on Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations. Office of the Secretary of Defence, Washington, D.C.

[2] M. Anderson, S. Martin, C. Dagli and A. Miller (2008). Implementing an Architectural Framework to Define and Deliver Net-Centric Capability to Legacy Military Air Assets Operating within a System of Systems, SysCon 2008, IEEE international Systems Conference, Montreal, Canada.

[3] A. Thomas, T. Turner and S. Soderlund (2008). Net-Centric Adapter for Legacy Systems, Military Communications Conference, San Diego, California.

[4] R. C. Brackney and R. H. Anderson (2004). Understanding the Insider Threat. Proceedings Corporation Conference, RAND National Security Research Division, Santa Monica, California.

[5] Cisco Systems (2008). Secure Network Analysis Essentials – Overview with Case Studies, Documentation, https://learningnetwork.cisco.com/docs/DOC-3710.html, last accessed on January 13, 2010.

[6] G. Lyon (1997). Network Mapper, Insecure.org documentation, http://nmap.org, last accessed on January 13, 2010.

[7] Tenable Network Security (2002). The Network Vulnerability Scanner, Documentation, http://nessus.org/nessus/, last accessed on January 13, 2010.

[8] O.Arkin, M.Kydyraliev, F. Yarochkin (2009). Xprobe2 Active OS Fingerprinting Tool, Documentation, http://xprobe.scourceforge.net, last accessed on January 13, 2010

[9] SolarWinds (1998). LANSurveyor, Documentation, http://www.solarwinds.com/products/LANsurveyor/, last accessed on January 13, 2010..

[10] F. Yarochkin, O. Arkin, M. Kydyraliev, S. Yao Dai, Y. Huang and S. Yen Kuo (2009). Xprobe2++: Low Volume Remote Network Information Gathering Tool, IEEE/IFIP International Conference on Dependable Systems & Networks, Lisbon, Portugal.

[11] M. Garuba, C. Liu and D. Fraites (2008). Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems, Fifth International Conference on Information Technology: New Generations, Section 6.6 Limitations of NIDS, Las Vegas, Nevada, USA.

[12] R. Henning (2003). Vulnerability Assessment in Wireless Networks, Symposium on Applications and the Internet Workshops 2003, Section 8.0 Architectural Options for RWAP Discovery and Analysis, Washington, DC, USA.

[13] M. Chad, B. Andrew, L. Qi, J. Yingxin, C. David, S. David and S. Aaron (2008). RIPPS: Rogues Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning, ACM Transactions on Information and System Security (TISSEC), Voume 11, Issue 2, Article No. 2, New York, USA.

[14] H. Hamed and E. Al-Shaer (2006). Taxonomy of Conflicts in Network Security Policies, IEEE Communications Magazine, Volume 44, Issue 3.

[15] Cisco (2007). Introduction to Cisco IOS NetFlow – A Technical Overview, Documentation, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html, last accessed on January 13, 2010.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia

2. Dudley Knox Library
Naval Postgraduate School
Monterey, California

3. Professor Geoffrey Xie
Department of Computer Science
Naval Postgraduate School
Monterey, California

4. Mr John Gibson
Department of Computer Science
Naval Postgraduate School
Monterey, Californi